BG ETEM Intranet Präventionswerkzeuge

Betriebshandbuch

Version	2.6
Stand:	08.02.2024
Autor:	Achim Müller
Ablage:	Betriebshandbuch_IPW.docx
Umfang:	57 Seiten

Versionshistorie

Version	Beschreibung	Autor	Datum
0.8	Dokument erstellt	Achim Müller	12.12.2014
0.9	Befunde aus Review eingearbeitet	Achim Müller	15.12.2014
1.0	Freigabe	Stefan Hofmaier	16.12.2014
1.1	Anpassungen für Windows-Installation	Felix Thiele	25.03.2015
1.2	Befunde eingearbeitet	Felix Thiele	16.04.2015
1.3	Aktualisierungen zu Release 1.5	Daniel Mager	21.07.2015
1.4	Review-Befunde eingearbeitet	Stefan Hofmaier	06.11.2015
1.5	GHS-Piktogramme (Symbole) beschrieben	Paul Parenko	07.12.2016
1.6	Aktualisierung & Freigabe für Release 1.7	Felix Thiele	30.12.2016
1.7	Erweiterung um Kapitel „Weitere bekannte Fehlersituationen und deren Behebung“	Felix Thiele	15.05.2017
1.8	Aktualisierung für Release 2.0	Felix Thiele	19.12.2017
1.9	Anpassung der Systemanforderungen für 64-Bit	Patrick Krings	17.07.2018
2.0	Anleitung des Migrationstools überarbeitet	Marcel Berger	14.05.2019

© BG ETEM 2024

2.1	Anmerkung zu Speicherplatz Anforderungen	Dominik Pham	26.05.2020
2.2	Überarbeitung für Release 2.4.1	Marcel Berger	29.06.2022
2.3	Überarbeitung für Release 2.4.1	Daniel Makarski	06.07.2022
2.4	Überarbeitung für Release 2.4.2	Marcel Berger	20.12.2022
2.5	Überarbeitung für Release 3.0.0	Daniel Makarski	24.10.2023
2.6	Anpassung Umgebungsspezifische Konfigurationen	Marcel Berger	08.02.2024
2.6a	Redaktionelle, allgemeine Anpassung	Sylke Pristat Martin Schröttke Axel Mühlthaler	11.03.2024

© BG ETEM 2024

Review

Version	Datum	Teilnehmer
0.8	13.12.2014	Stefan Hofmaier
1.3	06.11.2015	Stefan Hofmaier
1.7	17.05.2017	Stefan Hofmaier
1.8	20.12.2017	Stefan Hofmaier

© BG ETEM 2024

1 Inhaltsverzeichnis

1	**Inhaltsverzeichnis**	**5**
2	**Einleitung**	**7**
2.1	Zweck der Anwendung	7
2.2	Überblick zur Systemarchitektur	7
2.3	Systemvoraussetzungen für Client und Server	9
2.4	Erforderliche Kenntnisse der Administratoren	10
3	**Konfigurationsmöglichkeiten für die Systemkomponenten**	**11**
4	**Betrieb**	**12**
4.1	Beschreibung der Verzeichnisstruktur des Dateisystems	12
4.1.1	Hauptverzeichnis	12
4.1.2	Server-Applikation	12
4.1.3	Serverskripte	13
4.1.4	Datenbankskripte	13
4.1.5	Payara Domänenverzeichnis	14
4.1.6	ipw-config.xml	14
4.1.7	Mail-Vorlagen	14
4.1.8	Medienverzeichnis und Archiv	15
4.1.9	PDF-Vorlagen	16
4.1.10	Regelwerk	17
4.1.11	Client-Anwendung	18
4.2	Start und Stopp der Anwendung	18
4.3	Durchführung von Backup und Recovery	18
4.4	Beschreibung der Schnittstellen zu Umsystemen	19
4.4.1	LDAP-Server	19
4.4.1.1	Authentifizierung der Benutzer	19
4.4.1.2	Übernahme von Benutzerdaten	20
4.4.1.3	Konfiguration einer SSL-Verbindung zum LDAP-Server	23
4.4.2	E-Mail-Server	23
4.4.3	Terminversand	24
4.5	Beschreibung des DB-Schemas	25
4.6	Externer Link zum Erfassen von Verbandbucheinträgen	31
5	**Monitoring**	**32**
5.1	Verfügbarkeit der Anwendung	32

© BG ETEM 2024

5.2 Payara Application Server 32
5.3 Plattenplatz 33
5.4 Logfile-Archivierung und -Rotation 33
5.5 performance.csv 34
5.6 Payara-Server regelmäßig restarten 34

6 Fachliche administrative Aufgaben 36
6.1 Einspielen eines neuen Regelwerks 36
6.2 Etablieren einer neuen Sprache 36

7 Übernahme von Daten 38
7.1 Datenübernahme aus „Praxisgerechte Lösungen“ 38
7.2 Import von strukturierten Gefahrstoffdaten 40
7.3 Import von Dokumenten 40
7.4 Migration strukturierter Daten aus anderen Quellsystemen 41

8 Mögliche Fehlersituationen und deren Lösung 43
8.1 Fehlermeldungen in der Datei ipw.log 43
8.2 Glossar aller Fehlermeldungen 43
8.2.1 Fehlermeldungen des Backends (Server-Anwendung) 43
8.2.2 Fehlermeldungen des Frontends (Client-Anwendung) 53
8.3 Weitere bekannte Fehlersituationen und deren Behebung 55

9 Ansprechpartner bei nicht lösbaren Problemen 57

© BG ETEM 2024

2 Einleitung

2.1 Zweck der Anwendung

Die Deregulierung im Arbeitsschutzrecht hat den Unternehmen einerseits größere Gestaltungsspielräume im Arbeitsschutz gebracht, andererseits aber auch die Verpflichtung zu spezifischen Lösungen. Statt aus Vorschriften eindeutige Vorgaben ableiten zu können, hat der Unternehmer die Aufgabe, die betriebliche Situation zu betrachten und mögliche Gefahren zu beurteilen.

Die Gefährdungsbeurteilung als ideales Instrument zur Lösung dieser Aufgabe bietet neben der Reduzierung von Arbeitsunfällen, Berufskrankheiten und arbeitsbedingten Erkrankungen zusätzliche Möglichkeiten.

Angesichts des Interesses einer großen Zahl von Mitgliedsbetrieben der BG ETEM an einer webbasierten Datenbanklösung zur Gefährdungsbeurteilung hat die Abteilung Prävention der BG ETEM beschlossen, ihren Mittel- und Großbetrieben ein entsprechendes Werkzeug zur Verfügung zu stellen und dazu die vorhandene Lösung neu zu gestalten. Entsprechend der Software „Praxisgerechte Lösungen“, die sich in erster Linie an kleinere Betriebe wendet, soll ein leistungsfähiges Werkzeug die Unternehmen dabei unterstützen, mit dem Mittel Gefährdungsbeurteilung die Voraussetzungen zu gesundem und sicherem Arbeiten zu verbessern.

In der ersten Entwicklungsphase wurden Module der Arbeitsschritte 1 und 2 umgesetzt. Sie umfassen ein Modul zur **Gefährdungsbeurteilung** nach Gefahrstoffverordnung. Die erforderlichen Gefahrstoffinformationen werden im Modul **Gefahrstoffverzeichnis** erfasst und verwaltet. Ein **Betriebsanweisungseditor** sorgt dafür, die erforderlichen Dokumente und die Informationen an den einzelnen Arbeitsplätzen zu verbreiten. Eine umfangreiche **Regelwerkbibliothek** enthält die nötigen Quellen - externe und interne - die als Hintergrundinformation dienen.

Sollten Arbeitsplatzbeschreibungen bereits mit Hilfe der Software "Praxisgerechte Lösungen" erfasst worden sein, wird ein entsprechendes Werkzeug den **Migrationsprozess** unterstützen.

Ein differenziertes **Rechtekonzept** sorgt für einen an betriebliche Abläufe angepassten Workflow für Freigabe, Veröffentlichung und Administration.

In der zweiten Entwicklungsphase wurde u. A. das betriebliche Unfallmanagement in der Anwendung etabliert. Hiermit lassen sich Unfalldokumentationen erstellen, deren Informationsgehalt durch strukturierte Unfalluntersuchungen angereichert werden kann. Diese können Gefährdungsbeurteilungen zugeordnet werden und so zur Anpassung der Gefährdungsbeurteilung dienen.

2.2 Überblick zur Systemarchitektur

Bei der Anwendung „Intranet Präventionswerkzeuge“ handelt es sich um eine browserbasierte Lösung, mit der verschiedene Endanwender in ihrer Rolle als Administrator, Auswerter, Autor, Auftraggeber, Leser oder Ausführender arbeiten können.

Um den Anforderungen nach einer einfachen, intuitiven und attraktiven Benutzeroberfläche zu genügen wurde die Architekturform einer Rich Internet Applikation (RIA) gewählt. Hierbei wird die GUI mittels JavaScript/HTML5/CSS3 im Browser dargestellt und ermöglicht trotzdem eine Bedienbarkeit, wie man es von Desktop-Anwendungen gewohnt ist.

Die Benutzeroberfläche kommuniziert mittels einer REST-Schnittstelle mit dem Backend, das als Java EE 7-Anwendung in einem Application Server abläuft. Strukturierte Daten werden in einer relationalen Datenbank und große Binärdaten wie z. B. Mediendateien direkt im Dateisystem gespeichert.

An externen Systemen sind ein Verzeichnisdienst (LDAP) zur Authentifizierung der Benutzer und zum Auslesen von Benutzerdaten sowie ein Mail-Server (SMTP) zum Versand von Nachrichten und Terminen angebunden.

© BG ETEM 2024

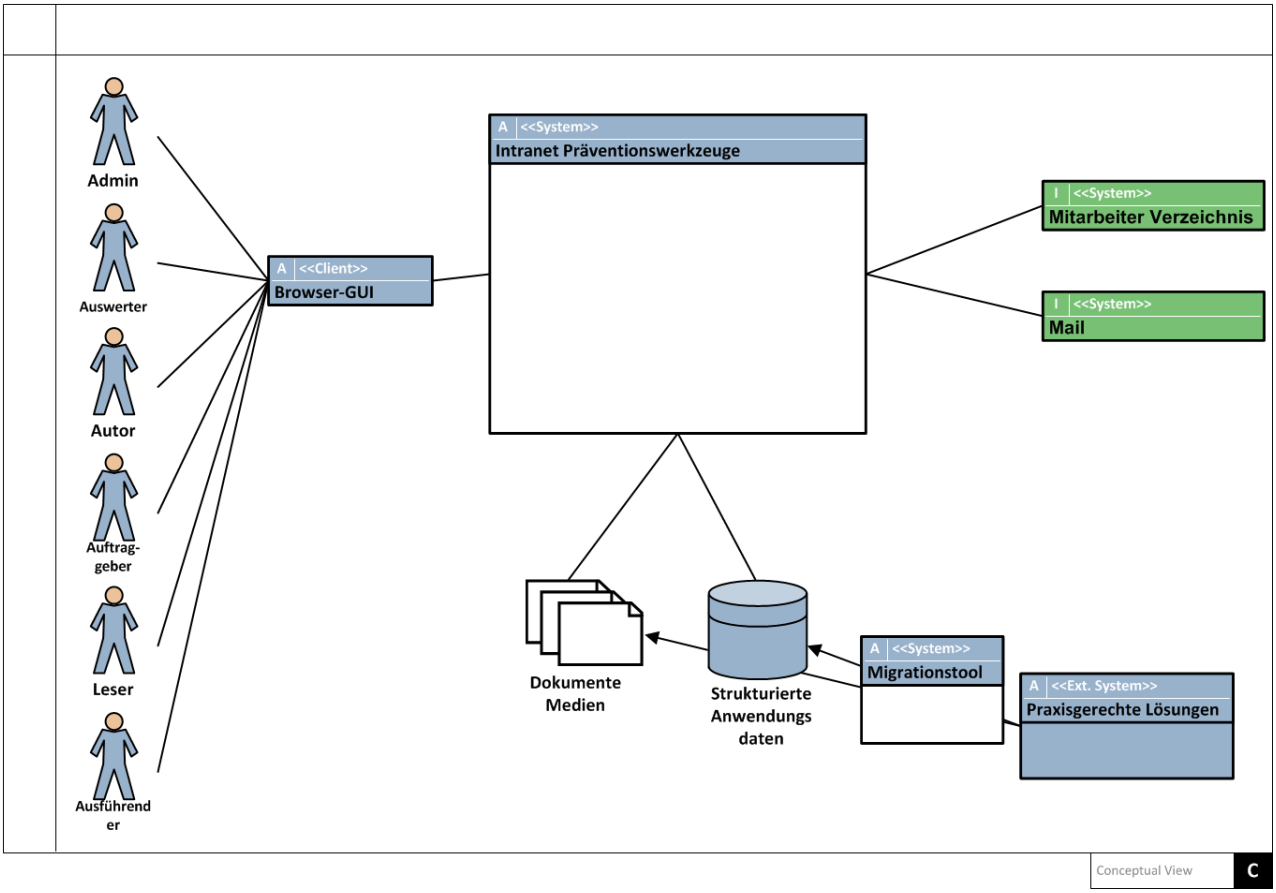


Abbildung 1: Kontext-Sicht auf die Anwendung "Intranet Präventionswerkzeuge"

Um dem zu erwartenden Lastprofil und der Anforderung nach einem möglichst hohen Anteil an lizenzkostenfreier Systemsoftware zu entsprechen, wurde serverseitig LINUX als Betriebssystem ausgewählt. Zusätzlich wird WindowsServer ab Version 2008 R2 unterstützt. Als Application Server kommt der Payara-Server zur Anwendung. Payara ist eine Weiterentwicklung des vormals verwendeten Glassfish-Servers, welcher neben regelmäßigen Aktualisierungen ebenfalls die Möglichkeit von kommerziellem Support bietet.

Um den Application Server von der Auslieferung der statischen HTML-Seiten bzw. JavaScript Code-Fragmenten zu entlasten, wird ein Apache Web Server vorgelagert. Die Http-Anfragen werden zuerst vom Apache Web Server entgegengenommen und dann bei Bedarf mittels des Moduls mod_proxy an den Payara-Server weitergegeben.

Die Java EE Anwendung innerhalb des Application Servers besteht grob aus 2 Modulen: Einem REST-API, das die Schnittstelle zum Frontend abbildet und innerhalb des Servlet-Containers ausgeführt wird, und einem Modul mit den implementieren Business-Funktionen, die als EJBs im EJB Container des Payara zur Ausführung kommen.

Beide Module greifen dabei auf bekannte Open Source-Frameworks wie Jersey, JAXB, Lucene, JavaMail und JPA/Hibernate etc. zurück.

© BG ETEM 2024

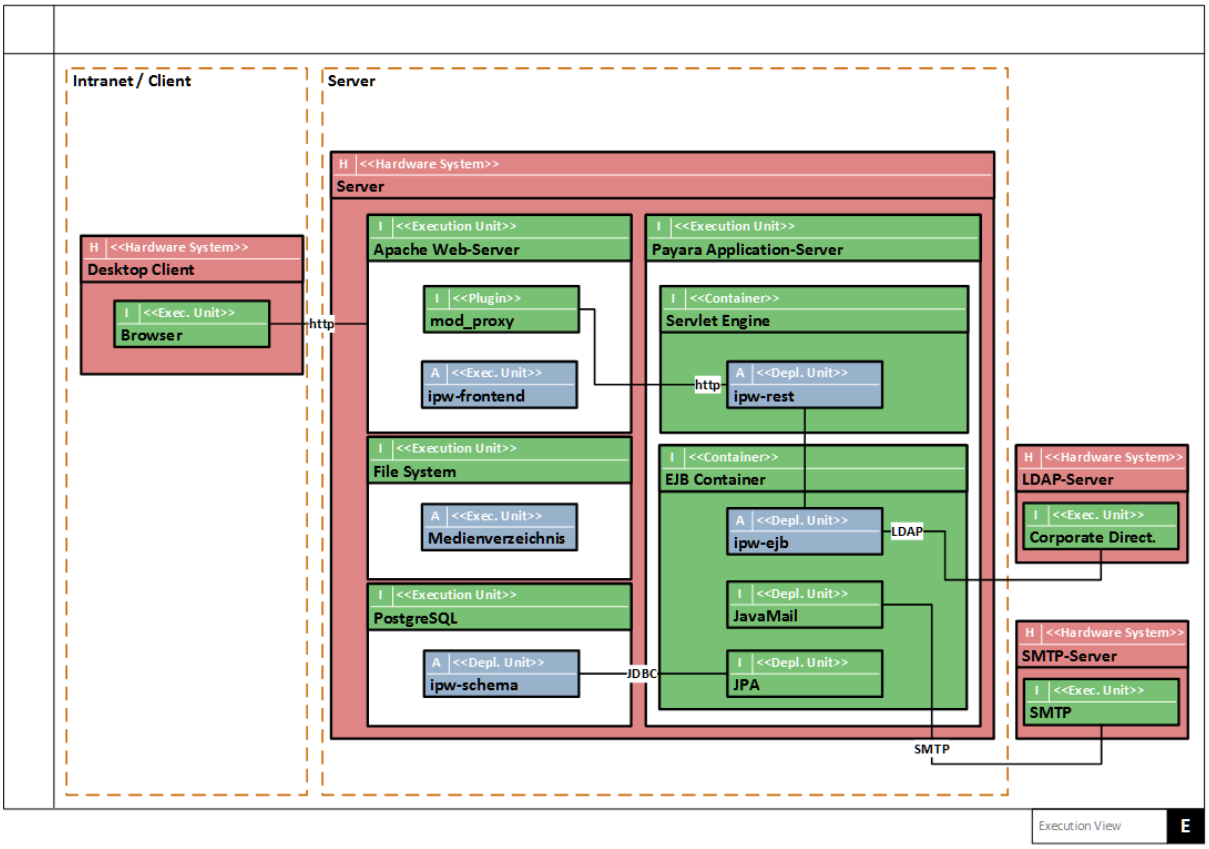


Abbildung 2: Ausführungssicht auf die Anwendung "Intranet Präventionswerkzeuge"

2.3 Systemvoraussetzungen für Client und Server

Für den Server-seitigen Betrieb der Anwendung „Intranet Präventionswerkzeuge“ gelten folgende Voraussetzungen:

Komponente	Version	Typ	Kommentar
Ubuntu Linux oder Microsoft Windows Server	16.04.3 oder höher 2008 R2 SP1 oder höher	Server-Betriebssystem	Die fehlerfreie Funktion auf anderen Linux Derivaten wird nicht garantiert 64-Bit Betriebssystem (ab Release 2.2) 2 GB RAM oder mehr
Apache	2.4.53 oder höher	Web Server	Auslieferung der Browser-Seiten
OpenJDK	8	Java Runtime	Java Runtime für Payara Application Server
Payara	4.1.2.181	Application Server	Laufzeitumgebung der Anwendung
PostgreSQL	14.2 oder höher	Datenbank	Datenspeicherung

Die Installation wurde erfolgreich unter Ubuntu 16.04.3 getestet. Grundsätzlich sollte aber jedes (aktuelle) Linux-Derivat möglich sein. Unter Windows wurde eine erfolgreiche Installation mit Windows Server 2008 R2 SP durchgeführt. Ab Release 2.2 der Intranet Präventionswerkzeuge wird aufgrund der aktualisierten Komponenten ein 64-Bit Betriebssystem als Systemanforderung vorausgesetzt. Der Apache Server sollte in der Version 2.4 oder höher vorliegen, da es für ältere Versionen keinen Support mehr gibt. Der Payara Server 4.1.2.181 benötigt eine Java 8 Runtime. Als Datenbank wurde PostgreSQL ausgewählt, da es sich hierbei um eine leistungsfähige, lizenzkostenfreie relationale Datenbank handelt.

Auf dem Client werden folgende Browser-Versionen unterstützt:

Browser	Version
Google Chrome	Ab Version 88
Firefox	Ab Version 85
Safari	Ab Version 14.5
Edge	Ab Version 85

Von der Verwendung des Browsers „Internet Explorer“ wird abgeraten, da dieser von „Intranet Präventionswerkzeuge 2“ nicht unterstützt wird.

2.4 Erforderliche Kenntnisse der Administratoren

Für die Installation und die Administration der Software sind fundamentale Linux- / UNIX- bzw. Windows-Kenntnisse **zwingend erforderlich**. Insbesondere sollten folgende Aufgaben ausgeführt werden können:

- Anlegen von Benutzern
- Anlegen von Verzeichnissen
- Berechtigungsvergabe
- Kopieren von Dateien
- Ausführen von Skripten
- Kenntnisse in der Installation von Software auf dem Zielsystem (z. B. YaSt unter OpenSUSE)

Für den Betrieb der Software sind Kenntnisse in der Administration und Konfiguration der folgenden Serversoftware erforderlich:

- Apache
- Payara
- PostgreSQL

Für die Pflege der Grunddaten sind **einfache SQL-Kenntnisse** erforderlich.

© BG ETEM 2024

3 Konfigurationsmöglichkeiten für die Systemkomponenten

Die Konfiguration der Systemkomponenten Apache, Payara und PostgreSQL ist ausführlich in der Installationsanleitung erläutert.

© BG ETEM 2024

4 Betrieb

Hinweis: Die in der Folge referenzierten Pfadangaben gelten für die Plattform **Linux**. Somit muss für die Plattform **Windows** der Separator „/“ gedanklich durch „\“ und die Dateiendung „.sh“ durch „.bat“ ersetzt werden.

4.1 Beschreibung der Verzeichnisstruktur des Dateisystems

4.1.1 Hauptverzeichnis

Das Hauptverzeichnis der Anwendung Intranet Präventionswerkzeuge liegt auf dem Server standardmäßig unter /var/ipw/ipw (Windows: C:\ipw\ipw). Darunter finden sich folgende Unterverzeichnisse:

Unterverzeichnis zu ipw	Beschreibung
app	Server-Applikation
bin	Server-Skripte
db	Datenbank-Skripte
gf.domains	Payara-Domäne
konfiguration	ipw-config.xml
mailvorlagen	E-Mail-Vorlagen
medien	Medienverzeichnis
pdfvorlagen	PDF-Vorlagen für Jasper Reports
regelwerk	Regelwerk der BG ETEM
symbole	GHS-Piktogramme (Symbole)
www	Client-Applikation

Für die Administration wichtig sind vor allem das /bin-Verzeichnis mit den Serverskripten und das /regelwerk-Verzeichnis, in dem aktualisierte Regelwerke einzuspielen sind.

Besondere Bedeutung hat das /medien-Verzeichnis, in das sämtliche Mediendateien, die von den Benutzern hochgeladen werden, abgespeichert werden.

4.1.2 Server-Applikation

Die Server-Applikation besteht aus einem Java Enterprise Archiv ipw.ear, welches im Payara-Server deployed wird.

Datei im Verzeichnis ipw/app	Beschreibung
ipw.ear	Server-Applikation

© BG ETEM 2024

4.1.3 Serverskripte

Für das Starten- und Stoppen der Serverinfrastruktur, das Anlegen und die Initial-Befüllung der Datenbank sowie für das Deployen der Anwendung im Payara-Server stehen im Verzeichnis ipw/bin vorbereitete Skripte zur Verfügung. Die Anpassung an die konkrete Umgebung mit ihren Installationspfaden erfolgt über das Skript setenv.sh, welches von allen Skripten benutzt wird.

Skript im Verzeichnis ipw/bin	Beschreibung
deploy.sh / deploy.bat	Deploy der Server-Applikation im Payara-Server
filldb.sh / filldb.bat	Löschen der Grunddaten und Einspielen von initialen Daten in die Datenbank
initdb.sh / initdb.bat	Löschen und neu anlegen des Datenbank-Schemas
redeploy.sh / redeploy.bat	Redeploy der Server-Applikation im Payara-Server (für den Fall dass diese bereits deployed war)
setenv.sh / setenv.bat	Setzte von umgebungsabhängigen Variablen wie den Pfad auf die Datenbank, Apache und Payara-Installation
startdb.sh / startdb.bat	Starten der Datenbank
startgf.sh / startgf.bat	Starten des Payara-Servers
startws.bat	Starten des Apache (nur auf Windows Installationen)
stopdb.sh / stopdb.bat	Stoppen der Datenbank
stopgf.sh / stopgf.bat	Stoppen des Payara-Servers
stopws.bat	Stoppen des Apache (nur auf Windows Installationen)

4.1.4 Datenbankskripte

Die Datenbankskripte werden von den Skripten initdb.sh und filldb.sh benutzt.

Skript im Verzeichnis ipw/db	Beschreibung
clean-db.sql	Leert den Inhalt aller Tabellen der Datenbank
import-auswahlliste-…sql	Skripte zum Einlesen der sprachabhängigen Auswahllisten mit Texten
import-grunddaten-…sql	Skripte zum Einlesen der Grunddaten (Benutzer, Rechte, Rollen, Startseitenelemente, etc.)
import-prod.sql	Hauptskript zum Einlesen der Auswahllisten und Grunddaten, inkludiert die anderen Skripte
schema-db.sql	Legt das Datenbank-Schema an
procedure.sql	Legt Stored Procedures für die Datenbank an

© BG ETEM 2024

schema.sql	Initialisiert das Datenbank-Schema samt Stored Procedures

4.1.5 Payara Domänenverzeichnis

Das Payara-Domänenverzeichnis wird bei der Installation manuell mit dem asadmin-Kommando angelegt. Im Folgenden werden nur die relevanten Unterverzeichnisse und Dateien beschrieben.

Datei im Verzeichnis ipw/gf.domains/ipw-domain	Beschreibung
/config/domain.xml	Hauptkonfigurationsdatei der Domäne
/config/logback.xml	Konfiguration der Protokollierung für ipw.log und performance.csv
/config/logging.properties	Konfiguration der Protokollierung für das server.log
/config/login.conf	Bindet das Login Modul der Anwendung „Intranet Präventionswerkzeuge“ ein
/logs	Verzeichnis für alle Logfiles, server.log, ipw.log und performance.csv inklusive deren History
/lib/ipw-sec-3.0.0.jar	Login-Modul für „Intranet Präventionswerkzeuge“
/lib/postgres-42.3.4.jar	JDBC-Treiber PostgreSQL-DB

4.1.6 ipw-config.xml

Die Datei ipw-config.xml ist die Hauptkonfigurationsdatei der Anwendung „Intranet Präventionswerkzeuge“. Änderungen an der Datei werden im laufenden Betrieb sofort wirksam. Mögliche Einstellungen sind in der Installationsanleitung detailliert beschrieben.

Datei im Verzeichnis ipw/konfiguration	Beschreibung
ipw-config.xml	Hauptkonfigurationsdatei der Anwendung „Intranet Präventionswerkzeuge“

4.1.7 Mail-Vorlagen

Mail-Vorlagen werden beim Erstellen der vom System zu versendenden E-Mails verwendet. Eine Vorlage besteht aus statischem Text und Platzhaltern, die beim Erstellen der E-Mail befüllt werden.

Datei im Verzeichnis ipw/mailvorlagen	Beschreibung
gv-statuswechsel-text.vm	Vorlage für die E-Mail, die beim Statuswechsel eines Gefahrstoffes verschickt wird
mail_freigabe_gefaehrdungsbeurteilung.vm	Vorlage für die E-Mail, welche bei Freigabe einer Gefährdungsbeurteilung an referenzierende Autoren versendet wird.

© BG ETEM 2024

mail_neue_unfallmeldung.vm	Vorlage für die E-Mail, welche bei Erzeugung einer Unfallmeldung an den entsprechenden Empfängerkreis versendet wird.
mail_neuer_verbandbucheintrag.vm	Vorlage für die E-Mail, welche bei Erzeugung eines Verbandbucheintrags an den entsprechenden Empfängerkreis versendet wird.
termin_durch_um.vm	Termin-Vorlage für VCALENDAR-Format für die E-Mail, die bei der Erzeugung einer Maßnahme aus einer Unfallmeldung verschickt wird.
termin_erinnerung.vm	Termin-Vorlage für VCALENDAR-Format für die E-Mail, die bei als Erinnerung zu Maßnahme aus einer Unfallmeldung verschickt wird.
termin_eskalation.vm	Termin-Vorlage für VCALENDAR-Format für die E-Mail, die bei Eskalation einer Maßnahme aus einer Unfallmeldung verschickt wird.
termin.vm	Termin-Vorlage für VCALENDAR-Format für die E-Mail, die aus der Aufgabenbearbeitung heraus verschickt werden kann.

4.1.8 Medienverzeichnis und Archiv

Im Medienverzeichnis werden alle vom System generierten und vom Benutzer hochgeladenen Dateien abgelegt. Die Ablage erfolgt nach Dokumenttyp in Unterverzeichnissen.

Unterverzeichnis im Verzeichnis ipw/medien	Beschreibung
/archiv	Verzeichnis, in dem Betriebsanweisungen im PDF-Format archiviert werden. Der Dateiname wird genauso gebildet wie normale Betriebsanweisungen (siehe ipw-config.xml) ergänzt um den Zeitstempel der Archivierung. Standardeinstellung: %anzeigename%.generiertebetriebsanweisung.%benutzerkennung%.%datumaenderung%.%datumerstellung%.%id%.%datumarchivierung%
/archiv/{gefaehrdungsbeurteilung_titel}	Unterverzeichnis, in dem eine Gefährdungsbeurteilung archiviert wird. Der Name des Unterverzeichnisses korrespondiert mit dem Titel der Gefährdungsbeurteilung. Darin enthalten sind die generierte Gefährdungsbeurteilung im PDF-Format und alle Anhänge und Verweise in Form von Dateien.
/{dokumenttyp}	Die Dateien des Medienverzeichnisses werden in Unterverzeichnissen nach Kategorie der Dokumente abgelegt. Die Namen der Kategorien sind in der Datei ipw-config.xml festgelegt (/Medienverwaltung/Fachlicher Typ).

© BG ETEM 2024

4.1.9 PDF-Vorlagen

Zur Generierung der PDF-Dokumente wurden Berichte in Jasper Reports erstellt. Die Berichte liegen in einer Quellversion und einer ausführbaren Version vor. Zur Laufzeit sind nur die ausführbaren Berichte relevant.

Unterverzeichnis bzw. Datei im Verzeichnis ipw/pdfvorlagen	Beschreibung
/source	Quelldateien der PDF Vorlagen für Jasper Reports
/source/ipw.properties **/source/ipw_de.properties** **/source/ipw_en.properties**	Enthalten die statischen Texte der PDF-Vorlagen in der jeweiligen Sprache. Für das Etablieren einer neuen Sprache muss eine neue .properties-Datei erstellt werden (Kapitel 6.2 Punkt 5)
Betriebsanweisung_arbeitsmittel.jasper **Betriebsanweisung_biostoffv.jasper** **Betriebsanweisung_gefahrstoff.jasper** **Betriebsanweisung_organisation.jasper** BetriebsanweisungArbeitsmittel_Subreport.jasper BetriebsanweisungArbeitsmittel_Subreport_Subreport.jasper BetriebsanweisungGefahrstoff_Subreport.jasper BetriebsanweisungGefahrstoff_Subreport_Subreport.jasper Betriebsanweisung_biostoffv_Subreport.jasper Betriebsanweisung_biostoffv_Subreport_Subreport.jasper Betriebsanweisung_organisation_Subreport.jasper Betriebsanweisung_organisation_Subreport_Subreport.jasper	Ausführbare PDF-Vorlagen für Betriebsanweisungen getrennt nach Typ (Arbeitsmittel, BioStoffV, Gefahrstoff, Organisation) mit verwendeten Subreports
Gefaehrdungsbeurteilung_Mainreport.jasper Gefaehrdungebeurteilung_Gefaehrdung.jasper Gefaehrdungsbeurteilung_Aufgabe.jasper Gefaehrdungsbeurteilung_Innen.jasper Gefaehrdungsbeurteilung_Massnahme.jasper gefaehrdungsbeurteilung_Verweisliste.jasper Gefaehrdungsbeurteilung_Verweisliste_Aufgabe.jasper Gefaehrdungsbeurteilung_Verweisliste_Gefaehrdung.jasper Gefaehrdungsbeurteilung_Verweisliste_Massnahme.jasper Gefaehrdungsbeurteilung__Subreport_Massnahme.jasper Gefaehrdungsbeurteilung__Subreport_Subreport.jasper Gefaehrdungsbeurteilung__Subreport_Subreport_Aufgabe.jasper Gefaehrdungsbeurteilung_Unfallmeldungen.jasper Gefaehrdungsbeurteilung_Risikobeurteilung Gefaehrdungsbeurteilung_Gefahrstoff.jasper Gefaehrdungsbeurteilung_Gefahrstoff_liste.jasper Gefaehrdungsbeurteilung_Gefahrstoff_Summe.jasper	Ausführbare PDF-Vorlagen für Gefährdungsbeurteilungen mit verwendeten Subreports
GefahrstoffEtikett_CLP3L_bis_50L.jasper **GefahrstoffEtikett_CLP_bis_3L.jasper** **GefahrstoffEtikett_CLP50L_bis_500L.jasper** **GefahrstoffEtikett_Kleinbehaelter.jasper** GefahrstoffEtikett_CLP3L_bis_50L_Saetze_Subreport.jasper GefahrstoffEtikett_CLP3L_bis_50L_Subreport.jasper	Ausführbare PDF-Vorlagen für Gefahrstoff-Etiketten getrennt nach Größe (Kleinbehälter, CLP bis 3L, CLP 3L bis 50L, CLP

Unterverzeichnis bzw. Datei im Verzeichnis ipw/pdfvorlagen	Beschreibung
GefahrstoffEtikett_CLP50L_bis_500L_Subreport.jasper GefahrstoffEtikett_CLP_bis_3L_Saetze_Subreport.jasper GefahrstoffEtikett_CLP_bis_3L_Subreport.jasper GefahrstoffEtikett_Kleinbehaelter_Subreport.jasper GefahrstoffEtikett_Unternehmendaten_Subreport.jasper	50L bis 500L) inklusive Subreports
Gefahrstoffverzeichnis_Report.jasper Gefahrstoffverzeichnis_Report_innen.jasper Gefahrstoffverzeichnis_Subreport_Frontpage.jasper Gefahrstoffverzeichnis_Subreport_liste.jasper Gefahrstoffverzeichnis_Subreport_Backpage.jasper	Ausführbare PDF-Vorlagen für den Gefahrstoffkataster
Reports_Von_Unfaellen.jasper	Ausführbare PDF-Vorlage für den Report von Unfalldokumentationen.
StrukturbaumKnoten_Komplett.jasper StrukturbaumKnoten_Subreport.jasper StrukturbaumKnoten_SubMainReport.jasper StrukturbaumKnoten_FrontPage.jasper StrukturbaumKnoten_Inhalt.jasper	Ausführbare PDF-Vorlagen für alle Gefährdungsbeurteilungen eines Strukturbaumknotens
Unfallanzeige.jasper	Ausführbare PDF-Vorlage für Unfallmeldungen.
Beinahe_Meldepflichig_ErsteHilfe.jasper Beinahe_Subreport.jasper Meldepflichtige_Unfaelle_Subreport.jasper Erste_Hilfe_Subreport.jasper	Ausführbare PDF-Vorlage für die globale Auswertung der Beinahe Unfälle, Meldepflichtigen Unfälle und Erste-Hilfe-Leistungen inklusive Subreports.
Beinahe_Unfaelle.jasper	Ausführbare PDF-Vorlage für die globale Auswertung der Beinahe Unfälle.
Meldepflichtige_Unfaelle.jasper	Ausführbare PDF-Vorlage für die globale Auswertung der Meldepflichtigen Unfälle.
Erste_Hilfe_Leistungen.jasper	Ausführbare PDF-Vorlage für die globale Auswertung der Erste-Hilfe-Leistungen.
Gefahrstoffmengen.jasper Gefahrstoffmengen_Subreport.jasper Gefahrstoffmengen_Subreport_Subreport.jasper	Ausführbare PDF-Vorlage für die globale Auswertung aller Gefahrstoffmengen inklusive Subreports.
1000_Mann_Quote.jasper	Ausführbare PDF-Vorlage für die globale Auswertung der 1000-Mann-Quote.

4.1.10 Regelwerk

Zum Regelwerk gehört ein Suchindex und, sofern es sich um eine neuere Version des Regelwerks handelt, ein Änderungsprotokoll.

ipw/regelwerk	Beschreibung
/changelog	Änderungsprotokoll für die Regelwerksaktualisierung; der Name ist fest vorgegeben und lautet changeLogRW.json.
/index	In diesem Verzeichnis wird der Suchindex für das Regelwerk abgelegt. Der Aufbau des Index erfolgt über die Funktion Verwaltung ➔ Regelwerk indexieren in der Anwendung.
/www	Das eigentliche Regelwerk im HTML-Format

4.1.11 Client-Anwendung

Die Dateien für die Anzeige im Browser liegen in diesem Ordner, von wo aus sie vom Apache ausgeliefert werden.

Dateien im Verzeichnis ipw/www	Beschreibung
/	HTML- und JavaScript-Dateien für Browserdarstellung
/assets/logo.png	Firmenlogo für GUI und PDF-Generierung

4.2 Start und Stopp der Anwendung

Für das Starten und Stoppen der Server stehen verschiedene Skripte im Verzeichnis ipw/bin zur Verfügung. Diese sind evtl. **vor der ersten Verwendung** an die lokale Installation **anzupassen** (insb. „setenv.sh“)

- setenv.* Setzen von Umgebungsvariablen
- startws.* / stopws.* Web Server (Apache) starten / stoppen (unter Windows)
- startgf.* / stopgf.* Payara-Server starten / stoppen
- startdb.* / stopdb.* Datenbank starten / stoppen

Für einen ordnungsgemäßen Betrieb der Anwendung ist der erfolgreiche Start von Apache, Payara und Datenbank zwingend erforderlich:

```
ipw/bin/startws.* (unter Windows)
ipw/bin/startgf.*
ipw/bin/startdb.*
```

Die Startreihenfolge ist unerheblich.

Es sollte sichergestellt werden, dass bei einem Start des Server-Rechners diese Systemkomponenten auch mitgestartet werden.

4.3 Durchführung von Backup und Recovery

Grundsätzlich müssen die Inhalte der Datenbank und des Medienarchivs mit allen Dateien gesichert werden. Hinzu kommt noch die aktuelle Systemkonfiguration. Diese Daten befinden sich standardmäßig alle im Verzeichnis /ipw. Im Einzelnen:

ipw/db - Datenbank

ipw/gf.domains - Payara-Konfiguration

© BG ETEM 2024

ipw/konfiguration - ipw-config.xml

ipw/medien - Medienarchiv

ipw/symbole - Symbolarchiv

ipw/unfallmedien - Unfalldateien

Wir empfehlen, das komplette ipw/-Verzeichnis zu sichern. Hierfür sind allerdings die PostgreSQL-Datenbank und damit der Payara-Server und Apache-Server zu stoppen.

Alternativ kann auch die Datenbank mit den entsprechenden Utilities der PostgreSQL-Datenbank gesichert werden. Eine ausführliche Dokumentation befindet sich hier:

http://www.postgresql.org/docs/9.3/interactive/backup.html

Backup der Datenbank in eine Ausgabedatei durchführen:

```
pg_dumpall > sicherungsdatei
```

Recovery der Datenbank aus der Backup-Datei durchführen:

```
psql -f sicherungsdatei ipwadmin
```

In diesem Fall sind die `Sicherungsdatei` und das Medien- und Symbolarchiv sowie die Konfiguration separat zu sichern.

4.4 Beschreibung der Schnittstellen zu Umsystemen

4.4.1 LDAP-Server

Der LDAP-Server wird für zwei Funktionen genutzt:

- Authentifizierung der Benutzer
- Auslesen von Benutzerdaten

Da für die Authentifizierung das LDAP-Modul des Payara-Servers verwendet wird, muss der LDAP-Server an zwei Stellen konfiguriert werden (domain.xml des Payara-Servers und ipw-config.xml).

4.4.1.1 Authentifizierung der Benutzer

Die Authentifizierung von Benutzern erfolgt in der Anwendung „Intranet Präventionswerkzeuge“ gegen einen unternehmensweiten LDAP-Server. In „Intranet Präventionswerkzeuge“ selbst erfolgt eine Passwortverwaltung nur für als „intern“ markierte Benutzer, die nicht gegen das LDAP abgeglichen werden.

Damit ein Benutzer aus dem LDAP Zugriffsberechtigung auf Module, Funktionen oder Knoten in der Unternehmensstruktur von „Intranet Präventionswerkzeuge“ erhalten kann, muss der Benutzer vorher in der Anwendung angelegt werden.

Die Erfassung und Pflege der Rollen und Anwendungsberechtigungen erfolgt ausschließlich innerhalb von „Intranet Präventionswerkzeuge“. Das LDAP dient nur zur Authentifizierung des Benutzers und zur Synchronisierung von Benutzerinformationen.

Die Authentifizierung gegen LDAP erfolgt immer in 2 Schritten:

- Eintrag des Benutzers im LDAP suchen
- Benutzer/Passwort gegen seinen Eintrag im LDAP authentifizieren

Je nachdem in welcher Reihenfolge diese Schritte durchgeführt werden, gibt es grundsätzlich 2 Verfahren:

1. Search-first (Zuerst suchen)
2. Authentication-first (Zuerst authentifizieren)

© BG ETEM 2024

Das Verfahren 1 ist nur möglich, wenn das LDAP so konfiguriert ist, dass ein anonymer Lesezugriff erlaubt ist. Andernfalls muss Verfahren 2 verwendet werden.

Verfahren 2 setzt voraus, dass ein technischer Benutzer für den Zugriff auf das LDAP konfiguriert und bekannt ist und ein anonymer Zugriff verboten wurde.

Da nicht bekannt ist, wie das LDAP in den Mitgliedsunternehmen konfiguriert ist, werden beide Verfahren unterstützt. Dies wird durch die Konfiguration folgender Parameter in der Datei domain.xml des Payara –Servers ermöglicht (siehe auch https://docs.oracle.com/cd/E19501-01/819-3658/ablpc/index.html und Installationsanleitung):

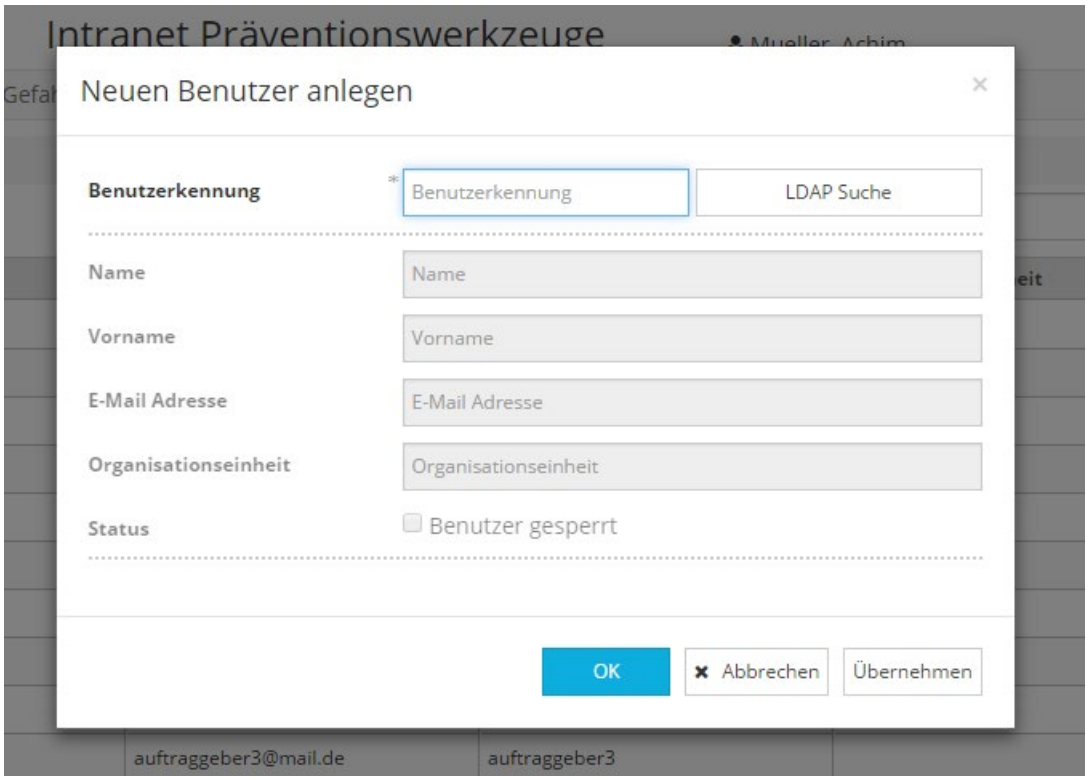
Parameter	Beschreibung	Beispiel
directory	LDAP-Server-URL mit Base DN	ldap://int.root.msg.ag:389
base-dn	Wurzelknoten zur Suche im Benutzerverzeichnis (im LDAP können grundsätzlich auch noch andere Informationen, z. B. Drucker, gespeichert werden)	DC=int,DC=root,DC=msg,DC=ag
jaas-context	Login-Modul, muss fix "IpwRealm" lauten	IpwRealm
search-filter	Suchfilter um Benutzereinträge im LDAP zu finden	(&(|(samAccountName=%s)(userPrincipalName=%s)(cn=%s))(objectClass=user))
search-bind-dn	Tech. Benutzer für die Anmeldung im LDAP mit Suchrechten	benutzer@int.root.msg.ag
search-bind-password	Passwort für techn. Benutzer	XYZ

Ist der Parameter "search-bind-dn" leer, wird Verfahren 1 angewendet, andernfalls Verfahren 2.

4.4.1.2 Übernahme von Benutzerdaten

Damit Benutzer Zugriff auf die Anwendung „Intranet Präventionswerkzeuge“ erhalten, muss für jeden Benutzer ein Benutzereintrag in der Anwendungsdatenbank vorhanden sein. Benutzer können von berechtigten Anwendern über den Menüpunkt "Verwaltung ➔ Benutzerverwaltung" erfasst werden. Nach Eingabe der Benutzerkennung können die zugehörigen Benutzerdaten wie Name, Vorname, E-Mail-Adresse und Organisationseinheit aus dem LDAP übernommen werden.

© BG ETEM 2024



Bei jedem erfolgreichem Login eines Benutzers gegen den LDAP-Server werden die Benutzerdaten aus dem LDAP-Verzeichnis ausgelesen und mit den für den Benutzer in „Intranet Präventionswerkzeuge“ gespeicherten Daten synchronisiert.

Für die Übernahme der Benutzerdaten aus dem LDAP ist eine Konfigurationsanpassung in der Datei ipw-config.xml erforderlich, z. B.:

```
<LDAP>
  <Server>ldap://servername:port</Server>
  <!-- Kommas sind mit \ zu escapen ! -->
  <BaseDN>dc=int\,dc=root\,dc=msg\,dc=ag</BaseDN>
  <Benutzerkennung>svc_ldap_ps@int.root.msg.ag</Benutzerkennung>
  <Passwort>Base64</Passwort>
  <BenutzerSuchFilter>
<![CDATA[(&(|(samAccountName={USERNAME})(userPrincipal-
Name={USERNAME})(cn={USERNAME})(sn={USERNAME}))(objectClass=user))]]>
  </BenutzerSuchFilter>
  <BenutzerSuchPlatzhalter>{USERNAME}</BenutzerSuchPlatzhalter>
  <SSL>true</SSL>
  <VerweiseFolgen>ignore</VerweiseFolgen>
  <BenutzerAttribute>
    <Benutzerkennung>samAccountName</Benutzerkennung>
    <Vorname>givenname</Vorname>
    <Nachname>sn</Nachname>
    <EMail>mail</EMail>
    <OrgaEinheit>department</OrgaEinheit>
    <KontoStatus gesperrt="514">userAccountControl</KontoStatus>
  </BenutzerAttribute>
</LDAP>
```

Feld	Mögliche Werte	Beschreibung
Server	LDAP URL	Adresse des LDAP-Servers in der Form ldap://server-name:port oder ldaps://servername:port (SSL)
BaseDN	Text	DN (Distinguished Name) des Startpunkts für Suchen im LDAP-Server; Kommas sind mit einem vorangestellten ‚\' zu kodieren. Beispiel: dc=xxx\,dc=yyy\,dc=zzz
Benutzerkennung	Text	Benutzerkennung für die Anmeldung am LDAP-Server, um Suchen durchführen zu können
Passwort	Text	Passwort der vorherigen Benutzerkennung verschlüsselt nach BASE64
BenutzerSuchFilter	Text	Suchfilter, um Benutzer im LDAP zu finden Beispiel: <![CDATA[(&(|(samAccountName={USERNAME})(user-PrincipalName={USERNAME})(cn={USER-NAME})(sn={USERNAME}))(objectClass=user))]]>
BenutzerSuchPlatzhalter	Text	Platzhalter für die Benutzerkennung im vorhergehenden Suchfilter Beispiel: {USERNAME}
SSL	true / false	Obsolet. SSL-Verbindung über das Protokoll-Präfix im Server-Feld konfigurieren (ldaps://)
VerweiseFolgen	follow, ignore, throw	Setzt java.naming.referral mit dem angegebenen Wert beim Verbindungsaufbau. Siehe auch https://docs.oracle.com/javase/jndi/tutorial/ldap/referral/jndi.html
BenutzerAttribute: Benutzerkennung	Text	Name des Attributes zum Auslesen der Benutzerkennung eines Benutzers. Diese muss dann auch beim Login angegeben werden und vom LDAP beim Login unterstützt werden. Bei ActiveDirectoy im Regelfall „samAccountName". Gebräuchlich ist auch „userPrincipalName".
BenutzerAttribute: Vorname	Text	Name des Attributes zum Auslesen des Vornamens eines Benutzers
BenutzerAttribute: Nachname	Text	Name des Attributes zum Auslesen des Nachnamens eines Benutzers
BenutzerAttribute: EMail	Text	Name des Attributes zum Auslesen der E-Mail-Adresse eines Benutzers

© BG ETEM 2024

BenutzerAttribute: OrgaEinheit	Text	Name des Attributes zum Auslesen der Organisationseinheit eines Benutzers
BenutzerAttribute: KontoStatus	Text und Zahl	Name des Attributes zum Auslesen des Status des Benutzerkontos; im XML-Attribut „gesperrt“ ist der Zahlenwert anzugeben, der ein gesperrtes Konto darstellt. Beispiel: <KontoStatus gesperrt="514">userAccountControl</KontoStatus>

Hinweis: Die Verschlüsselung des Passworts nach BASE 64 kann auf der Website https://www.base64encode.org/ vorgenommen werden.

4.4.1.3 Konfiguration einer SSL-Verbindung zum LDAP-Server

Eine SSL-Verbindung wird über das Protokoll-Präfix „ldaps://“ im <LDAP><Server> Element der ipw-config.xml und <directory> Element in der domain.xml konfiguriert. Der Standard-Port für ldaps ist 636.

Zusätzlich muss das entsprechende root-Zertifikat im Truststore der Payara-Domäne mit dem Java keytool hinzugefügt werden. Der IPW-Truststore befindet sich im Verzeichnis gf.domains\ipw-domain\config

Beispiel-Aufruf (Die Pfade sind gegebenenfalls anzupassen):

keytool -importcert -file company1.cer -alias company1 -keystore gf.domains/ipw-domain/config/cacerts.jks -storepass changeit

4.4.2 E-Mail-Server

Für den Versand von E-Mails muss ein SMTP-Server konfiguriert werden:

```
<Mail>
  <Server>zmr.msg.de</Server>
  <Port>25</Port>
  <AnmeldungErforderlich>false</AnmeldungErforderlich>
  <Benutzerkennung></Benutzerkennung>
  <Passwort></Passwort>
  <Absender>ipw@msg-systems.com</Absender>
  <AdminEmail>msg.projekt-ipw@msg-systems.com</AdminEmail>
  <TemplateVerzeichnis>/v/ipw/sw/var/qa/mailvorlagen</TemplateVerzeichnis>
  <UmleitungAktivAn>msg.projekt-ipw@msg-systems.com</UmleitungAktivAn>
</Mail>
```

Durch Füllen des Felds <UmleitungAktivAn> kann eine permanente Umleitung eingerichtet werden, damit auf einem Testsystem keine Mails an "echte" Benutzer versandt werden.

Feld	Mögliche Werte	Beschreibung
Server	DNS	DNS-Adresse des SMTP Servers
Port	Zahl	Port des SMTP Servers
AnmeldungErforderlich	true / false	Schalter, der angibt, ob für das Versenden von E-Mails eine Authentifizierung erforderlich ist.

© BG ETEM 2024

Benutzerkennung	Text	Benutzererkennung für die Anmeldung am SMTP-Server (falls AnmeldungErforderlich=true)
Passwort	Text	Passwort für die Anmeldung am SMTP-Server (falls AnmeldungErforderlich=true), BASE 64 kodiert
Absender	E-Mail-Adresse	Absender-Adresse von E-Mails, falls es keinen fachlichen Absender gibt, z. B. bei System-E-Mails
AdminEmail	E-Mail-Adresse	Empfänger E-Mail-Adresse für Systemmeldungen
TemplateVerzeichnis	Text	Verzeichnis, in dem die E-Mail-Vorlagen abgelegt sind
UmleitungAktivAn	E-Mail-Adresse	Empfänger E-Mail-Adresse, falls E-Mails zentral auf eine Adresse umgeleitet werden sollen, nur für Testsysteme sinnvoll. Ansonsten leer lassen.

4.4.3 Terminversand

Der Versand von Terminen lässt sich mittels Versand einer E-Mail mit einer .ics Datei als Anhang bewerkstelligen. Das .ics Dateiformat wird von den gängigen E-Mail-Programmen insbesondere auch von Lotus Notes unterstützt und bietet die Möglichkeit, Einzel- und Serientermine einzustellen.

Beispiel einer ICS-Datei:

```
BEGIN:VCALENDAR
VERSION:2.0
METHOD:PUBLISH
BEGIN:VTIMEZONE
TZID:W. Europe Standard Time
BEGIN:STANDARD
DTSTART:16011028T030000
RRULE:FREQ=YEARLY;BYDAY=-1SU;BYMONTH=10
TZOFFSETFROM:+0200
TZOFFSETTO:+0100
END:STANDARD
BEGIN:DAYLIGHT
DTSTART:16010325T020000
RRULE:FREQ=YEARLY;BYDAY=-1SU;BYMONTH=3
TZOFFSETFROM:+0100
TZOFFSETTO:+0200
END:DAYLIGHT
END:VTIMEZONE
BEGIN:VEVENT
CLASS:PUBLIC
CREATED:20140521T120121Z
DESCRIPTION:Dies ist der Text zum Termin.\n
DTEND;TZID="W. Europe Standard Time":20140520T130000
DTSTAMP:20140521T120122Z
DTSTART;TZID="W. Europe Standard Time":20140520T123000
LAST-MODIFIED:20140521T120121Z
LOCATION:München
PRIORITY:5
RRULE:FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR
SEQUENCE:0
SUMMARY;LANGUAGE=de:Beispieltermin
```

© BG ETEM 2024

TRANSP:OPAQUE
UID:040000008200E00074C5B7101A82E00800000000203ECE1CFD74CF01000000000000000
0100000005BBB420AB7D5E54CB2F0DD9CBD161A55
END:VEVENT
END:VCALENDAR

Um eine ICS-Datei zu generieren, sind folgende Parameter erforderlich:

Parameter	Beschreibung	Beispiel
SUMMARY	Betreff	Beispieltermin
DESCRIP-TION	Text des Kalendereintrags	Dies ist der Text zum Termin.
LOCATION	Ort	Köln
DTSTART	Start des Termins (20.05.2014, 12:30)	20140520T123000
DTEND	Ende des Termins (20.05.2014, 13:00)	20140520T130000
RRULE	Wiederholungsregel bei Serienterminen	WEEKLY;BYDAY=MO,TU,WE,TH,FR

4.5 Beschreibung des DB-Schemas

Das Datenbank-Schema, d.h. alle Tabellen mit ihren Feldern und Fremdschlüsselbeziehungen, wird über die Datei ipw/db/schema.sql angelegt.

Die einzelnen Felder sind in den Pflichtenheftdokumenten zum Domänenmodell beschrieben.

Tabelle	Inhalt	Beziehungen
BA_BETRIEBSANWEISUNG	Daten einer Betriebsanweisung	Rolle "besitzt Symbol" über BA_REL_BETRIEBSANWEISUNG_SYMBOL zu VW_SYMBOL
BA_REL_BETRIEBSANWEISUNG_SYMBOL	Symbole einer Betriebsanweisungen	Bildet die Rolle "besitzt Symbol" zwischen Betriebsanweisung und Symbol ab
GB_AUFGABE	Aufgaben	Rolle "gehört zu" Maßnahme in GB_MASSNAHME, Rolle "wird bearbeitet durch" Aufgabenbearbeitung in GB_AUFGABENBEARBEITUNG und Rolle "besitzt Auftragnehmer" und Rolle "besitzt Auftraggeber" zu Benutzer in VW_BENUTZER
GB_AUFGABENBEARBEITUNG	Aufgabenstatus	Rolle "gehört zu" Aufgabe in GB_AUFGABE
GB_BENUTZER_NODE_COLLAPSE_SETTING	Ansicht des Strukturbaums pro Nutzer	NodeCoollapseSetting „gehört zu“ Benutzer in VW_BENUTZER und „beschreibt“ den Zustand von Strukturbaumknoten in VW_STRUKTURBAUMKNOTEN

Tabelle	Inhalt	Beziehungen
GB_GEFAEHRDUNG	Gefährdungen einer Gefährdungsbeurteilung	Rolle "gehört zu" Gefährdungsbeurteilung in GB_GEFAEHRDUNGSBEURTEILUNG, Rolle "besitzt" Maßnahme in GB_MASSNAHME, Rolle "verursacht durch" Gefahrstoff in GV_GEFAHRSTOFF
GB_GEFAEHRDUNG_SORTIERUNG	Benutzersortierungen von Gefährdungen	benutzer_id gehört zu VW_BENUTZER und gefaehrdung_id zu GB_GEFAEHRDUNG
GB_GEFAEHRDUNG_SORTIERUNG_REIHENFOLGE	Speichert die Reihenfolge von Massnahmen der jeweiligen Gefährdungssortierung	massnahme_id gehört zu GB_MASSNAHME und gefaehrdung_sortierung_id zu GB_GEFAEHRDUNG_SORTIERUNG
GB_GEFAEHRDUNGSBEURTEILUNG	Gefährdungsbeurteilungen	Rolle "ist Verweisziel" von Verweis in VW_VERWEIS, Rolle "besitzt" Gefährdung GB_GEFAEHRDUNG, Rolle "besitzt" Schlüsselwort in GB_SCHLUESSELWORT über GB_REL_GEFAEHRDUNGSBEURTEILUNG_SCHLUESSELWORT, Rolle "hängt an" Strukturbaumknoten in VW_STRUKTURBAUMKNOTEN, Rolle "hat Datensatzverantwortlichen" als Benutzer in VW_BENUTZER
GB_GEFAEHRDUNGSBEURTEILUNG_SORTIERUNG	Benutzersortierungen von Gefährdungsbeurteilungen	benutzer_id gehört zu VW_BENUTZER und gefaehrdungsbeurteilung_id zu GB_GEFAEHRDUNGSBEURTEILUNG
GB_GEFAEHRDUNGSBEURTEILUNG_SORTIERUNG_REIHENFOLGE	Speichert die Reihenfolge von Gefährdungen der jeweiligen Gefährdungsbeurteilungssortierung	gefaehrdung_id gehört zu GB_GEFAEHRDUNG und gefaehrdungsbeurteilung_sortierung_id zu GB_GEFAEHRDUNGSBEURTEILUNG_SORTIERUNG
GB_GEFAEHRDUNGSFAKTOR	Gefährdungsfaktoren	Rolle "besitzt" Maßnahmenbaustein in GB_MASSNAHMEBAUSTEIN
GB_MASSNAHME	Maßnahmen zu einer Gefährdung	Rolle "gehört zu" Gefährdung in GB_GEFAEHRDUNG, Rolle "besitzt" Aufgabe in GB_AUFGABE
GB_MASSNAHME_SORTIERUNG	Benutzersortierungen von Massnahmen	benutzer_id gehört zu VW_BENUTZER und massnahme_id zu GB_MASSNAHME
GB_MASSNAHME_SORTIERUNG_REIHENFOLGE	Speichert die Reihenfolge von Aufgaben der jeweiligen Massnahmensortierung	aufgabe_id gehört zu GB_AUFGABE und massnahme_sortierung_id zu GB_MASSNAHME_SORTIERUNG

© BG ETEM 2024

Tabelle	Inhalt	Beziehungen
GB_MASSNAHMEBAUSTEIN	Maßnahmenbausteine zu einem Gefährdungsfaktor	Rolle "gehört zu" einem Gefährdungsfaktor in GB_GEFAEHRDUNGSFAKTOR
GB_PSA	Persönliche Schutzausrüstung	
GB_RISIKOBEURTEILUNG	Speichert Risikobeurteilungen von Gefährdungsfaktoren	gefaehrdung_id gehört zu GB_GEFAEHRDUNG und gefaehrdungsfaktor_id gehört zu GB_GEFAHRDUNGSFAKTOR
GB_REL_GEFAEHRDUNG_GEFAEHRDUNGSFAKTOR	Gefährdungsfaktoren einer Gefährdung	Stellt Rolle "Gefährdung besitzt Gefährdungsfaktoren" zwischen GB_GEFAEHRDUNG und GB_GEFAEHRDUNGSFAKTOR her
GB_REL_GEFAEHRDUNGSBEURTEILUNG_SCHLUESSELWORT	Schlüsselwörter einer Gefährdungsbeurteilung	Stellt Rolle "Gefährdungsbeurteilung besitzt Schlüsselwörter" zwischen GB_GEFAEHRDUNGSBEURTEILUNG und GB_SCHLUESSELWORT her
GB_REL_MASSNAHMEBAUSTEIN_GEFAEHRDUNGSFAKTOR	Maßnahmebaustein eines Gefährdungsfaktors	Stellt Rolle „Gefährdungsfaktor besitzt Maßnahmebausteine“ zwischen GB_GEFAEHRDUNGSFAKTOR und GB_MASSNAHMEBAUSTEIN her
GB_SCHLUESSELWORT	Schlüsselwörter	Rolle "gehört zu" Gefährdungsbeurteilung in GB_GEAFAEHRDUNGSBEURTEILUNG über GB_REL_GEFAEHRDUNGSBEURETILUNG_SCHLUESSELWORT
GV_GEFAHRENKLASSE	Gefahrenklasse eines Gefahrstoffes	Rolle "gehört zu" Gefahrstoff in GV_GEFAHRSTOFF
GV_GEFAHRSTOFF	Gefahrstoffe	Rolle "besitzt" Gefahrenklasse in GV_GEFAHRENKLASSE, Rolle "besitzt" Katastereintrag in GV_KATASTEREINTRAG, Rolle "besitzt" Satz in VW_SATZ über GV_REL_GEFAHRSTOFF_SATZ, Rolle "besitzt" Symbol in VW_SYMBOL über GV_REL GEFAHRSTOFF_SYMBOL
GV_KATASTEREINTRAG	Katastereinträge eines Gefahrstoffes	Rolle "gehört" zu Gefahrstoff in GV_GEFAHRSSTOFF
GV_REL_GEFAHRSTOFF_GEFAHRSTOFF	Gefahrstoffe eines Gemischs	Rolle „ist Bestandteil von“ Gefahrstoffen in GV_GEFAHRSTOFF
GV_REL_GEFAHRSTOFF_SATZ	Sätze eines Gefahrstoffes	Stellt Beziehung zwischen Gefahrstoff in GV_GEFAHRSTOFF und Satz in VW_SATZ her

© BG ETEM 2024

Tabelle	Inhalt	Beziehungen
GV_REL_GEFAHRSTOFF_SYMBOL	Symbole eines Gefahrstoffes	Stellt Beziehung zwischen Gefahrstoff in GV_GEFAHRSTOFF und Symbol in VW_SYMBOL her
MV_ARCHIVIERTE_DATEI	Dateien archivierter Gefährdungsbeurteilungen und Betriebsanweisungen.	
UM_BEARBEITUNGSTERMIN	Termine die durch Maßnahmen, welche aus Unfallmeldungen generiert werden, erzeugt werden. Ein Batch-Job läuft täglich über diese Tabelle und versendet Erinnerungen.	
UM_EMPFAENGERKREIS	Empfängerkreise für die Benachrichtigung bei neuen Unfallmeldungen / Verbandbucheinträgen.	Empfängerkreis „gehört zu“ Strukturbaumknoten in VW_STRUKTURBAUM
UM_REL_BENUTZER_EMPFAENGERKREIS	Benutzer in einem Empfängerkreis	Stellt Beziehung zwischen Empfängerkreis in UM_EMPFAENGERKREIS und Benutzer in VW_BENUTZER her
UM_REL_UNFALLMELDUNG_GEFAEHRDUNGSBEURTEILUNG	Gefährdungsbeurteilungen einer Unfallmeldung	Stellt Beziehung zwischen Unfallmeldung in UM_UNFALLMELDUNG und Gefährdungsbeurteilung in GB_GEFAEHRDUNGSBEURTEILUNG her
UM_REL_UNFALLMELDUNG_STRUKTURBAUMKNOTEN	Strukturbaumknoten einer Unfallmeldung	Stellt Beziehung zwischen Unfallmeldung in UM_UNFALLMELDUNG und Strukturbaumknoten in VW_STRUKTURBAUMKNOTEN her
UM_UNFALLANTWORTEN	Antwort zu einer Unfallfrage	Unfallantwort „gehört zu“ Unfallfrage in UM_UNFALLFRAGEN
UM_UNFALLANTWORTMOEGLICHKEITEN	Antwortmöglichkeiten einer Unfallantwort	Unfallantwortmöglichkeiten „gehört zu“ Unfallantwort in UM_UNFALLANTWORTEN
UM_UNFALLDATEI	Dateien, welche im Kontext einer Unfallmeldungen hochgeladen werden.	Unfalldatei „gehört zu“ Unfallmeldung in UM_UNFALLMELDUNG
UM_UNFALLDATEN	Daten bzgl. des Unfalls einer Unfallmeldung	Unfalldaten „gehört zu“ Unfallmeldung in UM_UNFALLMELDUNG
UM_UNFALLFRAGEBOGEN	Vorlagen für Unfallfragebogen inkl. ausgefüllter Unfallfragebögen.	Ausgefüllter Unfallfragebogen „gehört zu“ Unfallmeldung in UM_UNFALLMELDUNG

© BG ETEM 2024

Tabelle	Inhalt	Beziehungen
UM_UNFALLFRAGEN	Fragen	Unfallfrage „gehört zu“ Unfallfragebogen in UM_UNFALLFRAGEBOGEN
UM_UNFALLMELDUNG	Unfallmeldungen	
UM_UNFALLMELDUNGSYS-TEMDATEN	Systemdaten zu einer Unfallmeldung	Unfallmeldungsystemdaten „gehört zu“ Unfall-meldung in UM_UNFALLMELDUNG
UM_UNFALLNOTIZ	Unfallnotiz einer Unfall-meldung	Unfallnotiz „gehört zu“ Unfallmeldung in UM_UNFALLMELDUNG
UM_UNFALLUNTERSUCHUNGS-DATEI	Unfalluntersuchungsda-teien	Unfalluntersuchungsdatei „gehört zu“ Unfall-meldung in UM_UNFALLMELDUNG
UM_VERBANDBUCHEINTRAG	Verbandbucheinträge	
UM_VERBANDUCHPERSONENDA-TEN	Personendaten zu ei-nem Verbandbuchein-trag	Verbandbucheintragpersonendaten „gehört zu“ Verbandbucheintrag in UM_VERBANDBUCH-EINTRAG
UM_VERLETZTENANGABEN	Verletztenangaben zu einer Unfallmeldung	Verletztenangaben „gehört zu“ Unfallmeldung in UM_UNFALLMELDUNG
VW_AUSWAHLLISTE	Auswahllisten	Rolle "besitzt" Auswahllisteneintrag in VW_AUSWAHLLISTE_EINTRAG
VW_AUSWAHLLISTE_EINTRAG	Einträge einer Aus-wahlliste	Rolle "gehört zu" einer Auswahlliste in VW_AUSWAHLLISTE
VW_BENUTZER	Benutzer	Rolle "Verantwortlicher" einer Betriebsan-weisung in BA_BETRIEBSANWEISUNG oder Gefährdungsbeurteilung in GB_GE-FAEHRDUNGSBEURTEILUNG oder Ge-fahrstoff in GV_GEFAHRSTOFF, Rolle "Auftraggeber" oder "Auftragnehmer" ei-ner Aufgabe in GB_AUFGABE, Rolle "Zu-weiser" oder "Besitzer" eines Verweises in VW_VERWEIS, Rolle "Auslöser" eines Dokument-Logs in VW_DOKU-MENT_LOG, Rolle "berechtigt" für Kno-tenrolle in VW_BENUTZERKNOTEN-ROLLE, Rolle "besitzt" Startseitenelement in VW_DASHBOARDELEMENT über VW_REL_DASHBOARDELEMENT_ROL-LEBENUTZER
VW_BENUTZERBEARER	Vergebene „Bearer“-Tokens zum Spei-chern von Anmeldun-gen	Rolle "gehört zu" Benutzer in VW_BE-NUTZER
VW_BENUTZERKNOTENROLLE	Berechtigung eines Benutzers mit einer Rolle an einem Strukturbaumknoten	Verbindung zwischen VW_BENUTZER, VW_ROLLE und VW_STRUKTURBAUM-KNOTEN

© BG ETEM 2024

Tabelle	Inhalt	Beziehungen
VW_DASHBOARDELEMENT	Vorhandene Startseitenelemente	Zuordnung zu Benutzer oder Rolle über VW_REL_DASHBOARDELEMENT_ROLLEBENUTZER
VW_DATEI	Mediendateien	Rolle "Verweisziel" für Verweis in VW_VERWEIS
VW_DOKUMENT_LOG	Änderungsprotokoll auf Dokumente für das Dashboard	Rolle "Auslöser der Änderung" zu Benutzer in VW_BENUTZER
VW_MENGENEINHEIT	Mengeneinheiten	
VW_RECHT	Rechte	Rolle "gehört zu" Rolle in VW_ROLLE über VW_REL_ROLLE_RECHT
VW_REL_DASHBOARDELEMENT_ROLLEBENUTZER	Startseitenelemente eines Benutzers oder Rolle	Bildet Rolle "Benutzer hat Startseitenelement" zwischen VW_BENUTZER und VW_DASHBOARDELEMENTab
VW_REL_ROLLE_RECHT	Rechte einer Rolle	Bildet Rolle "Rolle besitzt Recht" zwischen VW_ROLLE und VW_RECHT ab
VW_ROLLE	Rollen	Rolle "ist Bestandteil einer" Benutzerknotenrolle in VW_BENUTZERKNOTENROLLE, Rolle "Besitzer eines" Startseitenelements in VW_DASHBOARDELEMENT, Rolle "besitzt" Recht von VW_RECHT, Rolle "Besitzer" eines Verweises aus VW_VERWEIS
VW_SATZ	Sätze	Rolle "gehört zu" Gefahrstoff in GV_GEFAHRSTOFF über GV_REL_GEFAHRSTOFF_SATZ
VW_STRUKTURBAUMKNOTEN	Strukturbaumknoten	Rolle "ist Vater von" einem anderen Strukturbaumknoten in VW_STRUKTURBAUMKNOTEN, Rolle "Anker" für Verweis in VW_VERWEIS, Rolle "Anker" für Gefährdungsbeurteilung in GB_GEFAEHRDUNGSBEURTEILUNG, Rolle "Bestandteil" einer Benutzerknotenrolle in VW_BENUTZERKNOTENROLLE
VW_STRUKTURBAUMKNOTENVERANTWORTLICHE	Verantwortliche eines Strukturbaumknotens, welche z. B. bei Eskalationen verwendet werden	Strukturbaumknotenverantwortlicher „gehört zu“ Strukturbaumknoten in VW_STRUKTURBAUMKNOTEN
VW_SYMBOL	Symbole	Rolle "gehört zu" Betriebsanweisung über BA_REL_BETRIEBSANWEISUNG_SYMBOL in BA_BETRIEBSANWEISUNG und Rolle "gehört zu" Gefahrstoff über

© BG ETEM 2024

Tabelle	Inhalt	Beziehungen
		GV_REL_GEFAHRSTOFF_SYMBOL in GV_GEFAHRSTOFF
VW_VERWEIS	Verweise	Rolle "hat Verweisquelle" Strukturbaumknoten in VW_STRUKTURBAUMKNOTEN, Rolle in VW_ROLLE und Benutzer in VW_BENUTZER, Rolle "hat Verweisziel" mit Datei in VW_DATEI und Gefährdungsbeurteilung in GB_GEFAEHRDUNGSBEURTEILUNG, mit Rolle "Zuweiser" zu Benutzer in VW_BENUTZER
AA_TERMIN	Termine des Moduls Übergeordnete Dokumente	Rolle "gehört zu" IPW-Objekt entweder in BA_BETRIEBSANWEISUNG, GB_GEFAEHRDUNGSBEURTEILUNG, GV_GEFAHRSTOFF, UM_UNFALLMELDUNG oder UM_VERBANDBUCHEINTRAG
AA_TERMINVERANTWORTLICHE	Verantwortliche eines Termins	Bildet Rolle „Benutzer ist verantwortlich für Termin“ zwischen VW_BENUTZER und AA_TERMIN ab
GV_GESTIS_INDEXTDATEI	Heruntergeladene Gestis-Stoffdatenbank	Keinerlei Beziehungen zu anderen Relationen
GV_GESTIS_ZEITDATEN	Metainformationen zur Gestis-Stoffdatenbank	Keinerlei Beziehungen zu anderen Relationen

Neben den fachlichen Attributen besitzen alle Tabellen die Spalten id und version. Die "id" ist ein technischer Schlüssel in Form einer fortlaufenden Nummer, die von der Datenbank generiert wird (Sequenz).

Die Spalte "version" wird benutzt, um konkurrierenden Schreibzugriff zweier Benutzer auf die gleiche Tabellenzeile zu entdecken (Optimistic Locking). Sie wird bei jedem Schreibzugriff vom JPA Persistenzframework automatisch hochgezählt.

4.6 Externer Link zum Erfassen von Verbandbucheinträgen

IPW unterstützt ab Release 2.0 die Erfassung von Verbandbucheinträgen. Dies ist auch für Benutzer möglich, die keinen Zugang zu IPW haben. Diese Funktion ist über einen externen Link erreichbar. Der externe Link zu IPW wird durch die Datei ‚external.html‘ ermöglicht. Diese HTML Datei ist nach Installation der Software im Apache DocumentRoot /var/ipw/www abgelegt und via Browser erreichbar.

Das Muster zur Erreichung des externen Links hat folgende Form:

http://*servername*/external.html

Der Servername von IPW obliegt dabei dem Betreiber. Eine Portangabe ist optional, wenn der Apache nicht unter http-Port 80 oder https-Port 443 betrieben wird.

Im Beispiel wurde IPW unter http auf ipw.msg.group deployed und der externe Link hätte folgende Form:

http://ipw.msg.group/external.html

© BG ETEM 2024

5 Monitoring

5.1 Verfügbarkeit der Anwendung

Um die Verfügbarkeit der Anwendung zu prüfen, kann regelmäßig die Seite

http://*servername*/ipw-rest/v1/vw/hallo

abgerufen werden. Wenn die Anwendung verfügbar ist, lautet er HTTP-Returncode „200 – OK“. Ein solcher sog. Healthcheck kann in vielen Monitoring-Tools mit einem definierten Intervall, z. B. minütlich, konfiguriert werden.

Natürlich kann die Seite auch manuell im Browser aufgerufen werden. Als Ausgabe erhält man Summenangaben für die wichtigsten fachlichen Objekte von „Intranet Präventionswerkzeuge“ im JSON-Format:

{"anzahlDateien":21,"anzahlGefahrstoffe":55,"anzahlGefaehrdungsbeurteilungen":14193,"anzahlStrukturbaumKnoten":4609,"anzahlVerweise":2446,"anzahlMassnahme":75671,"anzahlGefaehrdungen":14567,"anzahlAufgaben":75637,"anzahlBetriebsanweisungen":34,"anzahlBenutzer":176}

Der Vorteil dieser Seite besteht darin, dass alle 3 Serverkomponenten Apache, Payara-Server und die Datenbank aufgerufen werden.

5.2 Payara Application Server

Der Payara Application Server bietet ein eingebautes Monitoring mit vielen Einstellmöglichkeiten. Es funktioniert so, dass das Monitoring für eine Komponente des Servers explizit eingeschaltet und mit einem Monitoring Level LOW, MEDIUM oder HIGH versehen werden muss. Je nach Einstellung werden unterschiedliche viele Informationen gesammelt. Mögliche Server Komponenten sind:

- Web Container
- Thread Pool
- RESTFul Web Services
- JMS Service
- Web Services Container
- JPA
- Transaction Service
- JVM
- Security
- JDBC Connection Pool
- ORB
- Connector Connection Pool
- EJB Container
- Deployment
- Connector Service
- HTTP Service

Das Monitoring kann über die Admin Konsole konfiguriert und die gesammelten Informationen dort auch angezeigt werden. Es existiert aber auch eine Kommandozeilenschnittstelle.

Eine detaillierte Dokumentation ist unter diesem Link verfügbar (Kapitel 8. Administering the Monitoring Service):

https://docs.oracle.com/cd/E18930_01/html/821-2416/toc.html

Im normalen Produktivbetrieb muss das Monitoring des Payara Application Servers nicht aktiviert werden. Es dient eher dazu bei konkreten Problemen weitere Nachforschungen anstellen zu können. Solche Probleme können sein:

- Schlechtes Antwortzeitverhalten des Servers

© BG ETEM 2024

- Ressourcenknappheit (OutOfMemory-Meldungen)
- Fehlermeldungen beim Zugriff auf die Datenbank, die auf Knappheit bei den Datenbank-Verbindungen hindeuten

5.3 Plattenplatz

Da alle in die Intranet Präventionswerkzeuge hochgeladenen Dateien im Dateisystem unter

ipw/medien

abgelegt werden und auch der Upload von großen Dateien, z. B. Videodateien möglich ist, können hier beträchtliche Datenmengen zusammenkommen. Deswegen sollte der verfügbare Plattenplatz für dieses Verzeichnis regelmäßig überwacht werden.

Die Datenbank liegt standardmäßig unter

ipw/db/IPW_DATABASE

und benötigt nach der Migration aller Daten aus dem Vorgängersystem Praxisgerechte Lösungen ca. 100 MB.

Initial ist von einem Gesamtspeicherbedarf von 500 MB unter ipw/ ohne Installationspakete auszugehen.

Der Speicherbedarf wächst insbesondere durch die Anzahl der hochgeladenen Dateien ins Medienverzeichnis und die Logfiles (siehe nachfolgendes Kapitel). Die Maximalgröße der Logfiles beträgt in der aktuellen Konfiguration (14x100 MB + 14x1 MB = ca. 1,4 GB). Das Wachstum der Datenbank im laufenden Betrieb dagegen dürfte sich auf einige MB beschränken.

Um unerwartete Probleme aufgrund von Speicherengpässen entgegen zu wirken wird empfohlen, der Anwendung 50-70 GB an Speicherplatz zur Verfügung zu stellen.

5.4 Logfile-Archivierung und -Rotation

In der Standard-Konfiguration werden 3 Log-Dateien in das Verzeichnis

ipw/gf.domains/ipw_domain/logs

geschrieben:

- server.log
- ipw.log
- performance.csv

Das server.log wird vom Payara Server (Java Utils Logging) erstellt und in der Datei

ipw/gf.domains/ipw_domain/config/logger.properties

konfiguriert:

```
com.sun.enterprise.server.logging.GFFileHandler.rotationTimelimitInMinutes=1440
com.sun.enterprise.server.logging.GFFileHandler.rotationLimitInBytes=1000000
com.sun.enterprise.server.logging.GFFileHandler.maxHistoryFiles=14
```

Aktuell ist hier eine Log-Rotation alle 24h oder ab einer Dateigröße von 1 MB eingestellt. Es werden max. 14 Logfiles aufgehoben.

Die anderen beiden Logs iwp.log und performance.csv werden von der Applikation mittels des Logging Frameworks Logback geschrieben und zentral in der Datei

ipw/gf.domains/ipw_domain/config/logback.xml

konfiguriert (Auszug):

```
<rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
  <fileNamePattern>../logs/ipw.%d{yyyy-MM-dd}.%i.log</fileNamePattern>
```

```
  <maxHistory>14</maxHistory>
  <timeBasedFileNamingAndTriggeringPolicy class="ch.qos.logback.core.rolling.SizeAndTime-
BasedFNATP">
    <maxFileSize>100MB</maxFileSize>
  </timeBasedFileNamingAndTriggeringPolicy>
</rollingPolicy>
```

Da die Applikation wesentlich mehr Einträge schreibt, ist die maximale Dateigröße standardmäßig mit 100 MB definiert. Es werden 14 Dateien aufgehoben. Eine ausführliche Dokumentation der Konfigurationsmöglichkeiten findet sich unter:

http://logback.qos.ch/manual/index.html

Die Datei ipw.log ist die Hauptinformationsquelle für Applikationsfehler. Die Datei performance.csv dient ausschließlich für Performance-Analysen und kann auch temporär abgeschaltet werden.

Möchte man auch Fehler nachvollziehen können, die länger als 14 Tage zurückliegen, so sollten auch die Logfiles gesichert werden.

5.5 performance.csv

Diese spezielle Log-Datei dient zum Protokollierung des Antwortverhaltens und Performanz der Anwendung. Es handelt sich um eine CSV-Datei, die z.B. mit Excel geöffnet werden kann. Die einzelnen Spalten bedeuten:

- Zeitstempel
- Benutzerkennung
- Session ID
- Aktion: START/END/CALL
- Service-Name
- Benötigte Zeit in ms (nur END)
- Service-Parameter/Rückgabewerte

Mögliche Aktionen:

START	- Beginn der Ausführung der Service-Methode
END	- Ausführung der Service-Methode beendet
CALL	- Es wird nur der Aufruf der Service-Methode protokolliert (ohne Beginn und Ende)

Beispiel:

```
21-11-2014_12:59:25.732;huberc;MTQxNjU3MTE2NjM0M25pY2h0ZXJs-
ZWRpZ3RlYXVmZ2FiZW4xNQ==;END;DashboardResource.nichtErledigteAufgaben;40;200: 19
Entities gefunden
```

Der Aufruf der Service-Methode "DashboardResource.nichtErledigtAufgaben" durch Benutzer "huberc" benötigte am 21.11.2014 um 12:59:25 ein Zeitspanne von 40ms. Dabei wurden 19 Datenbankeinträge gefunden.

5.6 Payara-Server regelmäßig restarten

In der Entwicklungsphase der Anwendung „Intranet Präventionswerkzeuge“ kam es sporadisch zu folgendem Serverfehler:

Im server.log:

```
java.lang.OutOfMemoryError: Heap Space
```

In diesem Fall muss der Payara-Server neu gestartet

```
stopgf.sh/startgf.sh
```

und ein Deploy der Applikation ausgelöst werden.

`deploy.sh`

© BG ETEM 2024

6 Fachliche administrative Aufgaben

6.1 Einspielen eines neuen Regelwerks

Das von der BG ETEM bereitgestellte Regelwerk besteht aus einer Sammlung von HTML-Dateien und einem Änderungsprotokoll. Das Änderungsprotokoll ist eine Datei im JSON-Format mit dem festen Namen

changeLogRW.json

In dieser Datei wird festgehalten, welche Seiten in der vorliegenden Version im Vergleich zur letzten Version gelöscht, umbenannt oder an eine andere Stelle verschoben wurden, damit in der Anwendung „Intranet Präventionswerkzeuge“ Verweise auf solche Regelwerksseiten aktualisiert werden können. D. h. es muss sichergestellt werden, dass alle Versionen des Regelwerks auch kontinuierlich eingespielt wurden, da sich die changeLogRW.json sonst auf die falsche Vorgängerversion bezieht.

Ablageort:

ipw/regelwerk/www	- HTML-Dateien
ipw/regelwerk/changelog	- Änderungsprotokoll

Bei der Anlieferung eines neuen Regelwerks ist wie folgt vorzugehen:

1. Altes Regelwerk löschen/sichern

   Die alten Regelwerksseiten unter ipw/regelwerk/www sollten gesichert und anschließend gelöscht werden, damit keine Vermischung von alten und neuen Seiten stattfindet.

2. Neue Dateien nach ipw/regelwerk/www kopieren bzw. extrahieren
3. Änderungsprotokoll nach /var/ipw/regelwerk/changelog kopieren

Nach dem Einspielen der neuen Regelwerks-Version sollte man sich in der Anwendung „Intranet Präventionswerkzeuge“ anmelden und im Modul Regelwerk kontrollieren, ob die neuen Seiten angezeigt werden. Evtl. ist der Browsercache zu leeren! Danach sollten in der Anwendung von berechtigten Anwendern folgende Prozesse gestartet werden:

4. Menüpunkt "Verwaltung ➔ Regelwerk indexieren"

   Aktualisiert die Suchindizes.

5. Menüpunkt "Verwaltung ➔ Regelwerk aktualisieren"

   Aktualisiert Verweise laut Änderungsprotokoll.

6. Menüpunkt "Verwaltung ➔ Regelwerk" und dann Schaltfläche "Linküberprüfung starten"

   Listet fehlerhafte Links auf.

6.2 Etablieren einer neuen Sprache

Um eine neue Sprache in der Anwendung zu etablieren sind mehrere Schritte durchzuführen:

1. In der Sprachverwaltung der Anwendung (nur verfügbar mit dem Recht „Sprachen Verwalten“ im Menü Verwaltung) muss eine neue Sprache angelegt werden und eine bestehende Sprache als „Vorlage“ ausgewählt werden. Dies führt dazu, dass auf dem Server im Verzeichnis /var/ipw/ipw/www/app eine neue Datei x-translation.json erzeugt wird, wobei x das Sprachkürzel der neuen Sprache ist und unter /var/ipw/ipw/www/help ein neuer Ordner mit dem Namen des Sprachkürzels
2. Die x-translation.json kann mit einem Texteditor geöffnet werden und die darin enthaltenen Texte übersetzt werden. Wichtig ist, dass lediglich die „Values“, d.h. die Werte hinter einem Doppelpunkt übersetzt werden. Die „Keys“ vor dem Doppelpunkt müssen unverändert belassen werden.

© BG ETEM 2024

3. Um die Online-Hilfe zu übersetzen, muss die HTML Datei innerhalb des neu generierten Ordners /var/ipw/ipw/www/help/x/help.html mit einem Texteditor geöffnet werden und alle darin enthaltenen Texte übersetzt werden. Wichtig ist, dass die Verwendeten HTML-Tags, bzw. die Attribute dieser, unverändert bleiben, da ansonsten Verlinkungen o.ä. nicht mehr funktionieren. Außerdem sind die im Ordner img enthaltenen Bilder zu erneuern.
4. Innerhalb der Anwendung sind über das Verwaltungsmodul „Auswahllisten verwalten“ die im System hinterlegten Auswahllisteneinträge zu übersetzen.
5. Damit die in der Anwendung erzeugten PDF-Dokumente ebenfalls übersetzt sind, muss im Verzeichnis /var/ipw/ipw/pdfvorlagen/source eine .properties-Datei als Vorlage ausgewählt und eine neue Datei ipw_x.properties erstellt werden, wobei x das Sprachkürzel der neuen Sprache ist. Die ipw_x.properties-Datei kann ebenfalls mit einem Texteditor geöffnet werden und die enthaltenen Texte übersetzt werden. Wichtig ist, dass nur die „Values“, d.h. Werte nach dem „=“-Symbol, angepasst werden. Die “Keys“ vor dem „=“-Symbol müssen unverändert bleiben.

© BG ETEM 2024

7 Übernahme von Daten

Mitgliedsunternehmen können bestehende Gefährdungsbeurteilungen, Betriebsanweisungen und Gefahrstoffdaten nach „Intranet Präventionswerkzeuge“ übernehmen. Hierfür gibt es verschiedene Möglichkeiten:

- Datenübernahme aus „Praxisgerechte Lösungen“
- Import von strukturierten Gefahrstoffdaten
- Import von bestehender Betriebsanweisungen und Gefährdungsbeurteilungen als pdf-Dokumente
- Migration strukturierter Daten aus anderen Quellsystemen

Die folgenden Kapitel geben einen kurzen Überblick zu den einzelnen Möglichkeiten der Datenübernahme.

7.1 Datenübernahme aus „Praxisgerechte Lösungen“

Die Anwendung „Intranet Präventionswerkzeuge“ wird mit einem Migrationswerkzeug ausgeliefert, das die automatisierte Datenübernahme aus Katalogen von „Praxisgerechte Lösungen“ nach „Intranet Präventionswerkzeuge ermöglicht.

Folgende Objekte aus „Praxisgerechte Lösungen“ werden dabei berücksichtigt:

- Der Strukturbaum
- Benutzer
- Benutzerrechte
- Gefährdungsbeurteilungen inkl. der dafür erfassten Maßnahmen und Aufgaben
- Links und Dateien

Voraussetzung für die Datenübernahme ist, dass der Katalog (bek-Datei) aus der Version 4 von „Praxisgerechte Lösungen“ stammt.

Abbildung 3: Datenübernahme aus "Praxisgerechte Lösungen"

Für die Datenübernahme gelten die folgenden Regeln:

- Die obersten Knoten des Strukturbaums unterhalb des Katalognamens aus „Praxisgerechte Lösungen“ werden entweder unterhalb des Wurzelknotens in „Intranet Präventionswerkzeuge“ oder unter einem neuen Knoten angelegt. Um einen neuen Knoten bei der Migration zu erstellen, kann vorher ein Knotenname in der migration.properties-Datei konfiguriert werden. Sie können die Knoten auch im Nachgang über die Funktionsschaltflächen „Ausschneiden“ und „Einfügen“ des Dialogs „Strukturbaum verwalten“ an andere Stellen des Strukturbaums verschieben.
- Es werden nur Benutzerkürzel nach Intranet Präventionswerkzeuge übernommen, die im Verzeichniskatalog (LDAP) des Unternehmens vorhanden sind.
- Abhängig von den in „Praxisgerechte Lösungen“ vorhandenen Nutzerrechten wird jedem übernommenen Benutzer entweder die Rolle „Leser“ oder die Rolle „Autor“ am Wurzelknoten von „Intranet Präventionswerkzeuge“ zugeordnet. Optional kann vor der Migration in der migration.properties-Datei die Admin-Zuordnung eingeschaltet werden. Dabei werden keine Benutzer und Rollen aus „Praxisgerechte Lösungen“ übernommen.

© BG ETEM 2024

Stattdessen erhalten die Standard-Administratoren von „Intranet Präventionswerkzeuge“ den Zugriff auf den Wurzelknoten mit der Rolle „Administrator“

- Die Einschränkung von Nutzerrechten kann in „Intranet Präventionswerkzeuge“ nicht abgebildet werden und wird deshalb nicht übernommen.
- Für jede Maßnahme ohne konkrete Aufgabe wird in „Intranet Präventionswerkzeuge“ automatisch eine Aufgabe angelegt. Diese Funktion kann durch die Konfiguration in der migration.properties-Datei vor der Migration ebenfalls aus-/angeschaltet werden
- Links aus Gefährdungsbeurteilungen oder Maßnahmen in den BG-Katalog können in „Intranet Präventionswerkzeuge“ nicht abgebildet werden und werden deshalb nicht übernommen.

Das Migrationswerkzeug protokolliert alle während der Datenübernahme festgestellten Auffälligkeiten in einer Datei. Die dort protokollierten Meldungstypen sind im Dokument 100b_Glossar Meldungen Migrationswerkzeug.pdf beschrieben.

Das Migrationswerkzeug wird über folgende Befehle gestartet:

unter Windows:

```
cd <Installationsverzeichnis>\ipw\migration[1]
windows-migration.bat
```

unter Linux:

```
cd <Installationsverzeichnis>/ipw/migration
sh linux-migration.sh
```

Die zu migrierende bek-Datei sowie weitere für die Ausführung des Migrationswerkzeugs erforderliche Daten, werden in der Datei migration.properties hinterlegt.

Nachfolgend ein beispielhafter Inhalt einer migration.properties Datei:

```
#Basiseinstellungen
server_dns=ipw.msg.de
server_port=8037
deployed_app_name=ipw/ipw-ejb-3.0.0
#Zu migrierende Datei
database_path=F:/pgl/pglmsg.bek
#Import-Schlater
benutzer_gegen_ldap_verifizieren=true
```

Das Migrationstool kann optional auch direkt mit Java aufgerufen werden. Die Ausführung erfolgt durch folgenden Befehl:

```
java –jar ipw-mig-<Version>.jar migration.properties[2]
```

Für den Start des Migrationswerkzeugs gelten folgende Voraussetzungen:

- Die jar-Datei des Migrationswerkzeugs muss vor dem Start der Migration vom Installationsverzeichnis auf dem Server aus dem Unterverzeichnis „Migration“ auf den Zielrechner kopiert werden. Da in Gefährdungsbeurteilungen ggf. Links auf Dateien, die sich auf Netzwerklaufwerken befinden, referenziert werden, ist es sinnvoll, als Zielrechner einen Windows-Rechner zu verwenden.

[1] <Installationsverzeichnis> wird entsprechend durch das Installationsverzeichnis von Intranet Präventionswerkzeuge ersetzt (standardmäßig C:/ipw unter Windows und /var/ipw unter Linux)

[2] <Version> wird entsprechend durch die Version des Migrationstools ersetzt (Beispiel: ipw-mig-2.3.jar)

- Auf dem Zielrechner wird eine Java Runtime Version 8. benötigt. Im Rahmen der Installation von Intranet Präventionswerkzeuge wird eine entsprechende Java Runtime mit ausgeliefert. Für die Migration sollte die Java Executeable der mitgelieferten Java Runtime verwendet werden, welche im Installationsverzeichnis unter jre/bin zur Verfügung steht.
- Der Rechner, auf dem das Migrationswerkzeug ausgeführt wird, sollte Zugriff auf die in Gefährdungsbeurteilungen und Maßnahmen referenzierten Dateien haben. Die hierfür erforderlichen Pfade können aus den Fehlermeldungen in der Protokolldatei nach Durchführung einer ersten Testmigration ermittelt werden.
- Der Server muss von dem Rechner, auf dem das Migrationswerkzeug ausgeführt wird, auf dem RMI-Port (Default: 8037) erreichbar sein. Evtl. muss dieser hierfür temporär in der Firewall freigeschaltet werden.
- Vor dem Start des Migrationswerkzeugs müssen die erforderlichen Einstellungen in der Datei migraton.properties gesetzt werden.

7.2 Import von strukturierten Gefahrstoffdaten

Die Anwendung „Intranet Präventionswerkzeuge wird mit einem Werkzeug ausgeliefert, das den automatisierten Import von Gefahrstoffdaten ermöglicht. Mitgliedsunternehmen, die bereits über ein Gefahrstoffverzeichnis verfügen und die dort vorhandenen Daten nach „Intranet Präventionswerkzeuge“ übernehmen möchten, müssen diese Daten hierfür im Format csv in einer definierten Verzeichnisstruktur zur Verfügung stellen. Form, Inhalte und Struktur der bereitzustellenden Dateien sowie der Aufruf des Gefahrstoff-Imports sind in dem Dokument GefahrstoffImport.docx beschrieben.

Folgende Daten können bei dem Import nach „Intranet Präventionswerkzeuge“ übernommen werden:

- Stoffdaten
- Sätze
- Lagerorte und –mengen
- Dokumente, z. B. Sicherheitsdatenblätter oder Berichte

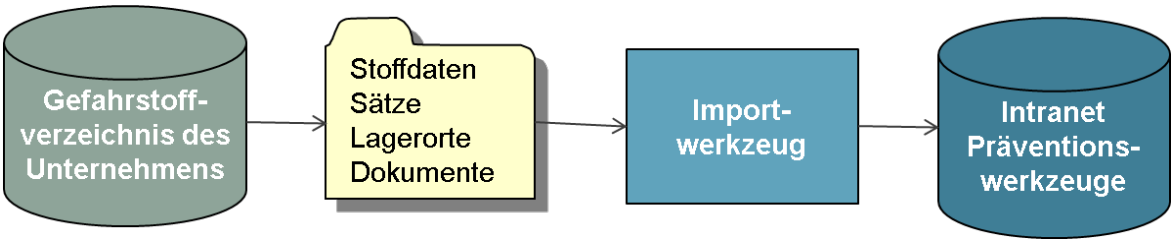


Abbildung 4: Import von strukturierten Gefahrstoffdaten

7.3 Import von Dokumenten

Die Anwendung „Intranet Präventionswerkzeuge“ bietet die Möglichkeit, Dateien im sog. Medienverzeichnis zu verwalten und mit Gefahrstoffen und Gefährdungsbeurteilungen zu verknüpfen. Die Dateien werden im Medienverzeichnis nach der Dokumentenkategorie strukturiert. So gibt es z. B. Kategorien für Gefährdungsbeurteilungen, Musterbetriebsanweisungen oder Unterweisungsberichte.

Dies eröffnet den Mitgliedsunternehmen die Möglichkeit, bestehende und in Dokumentenform verfügbare Gefährdungsbeurteilungen, Betriebsanweisungen oder Berichte in das Medienverzeichnis zu importieren und sie anschließend als Verweis mit Gefährdungsbeurteilungen, die in „Intranet Präventionswerkzeuge“ angelegt wurden, zu verknüpfen.

Der Import solcher Dokumente kann von berechtigten Nutzern über den Verweis-Manager von „Intranet Präventionswerkzeuge“ durchgeführt werden. Der Verweismanager kann entweder über die Funktion „Lesezeichen zuordnen“ oder über das Hinzufügen von Verweisen zu Gefährdungsbeurteilungen, Maßnahmen oder Aufgaben gestartet werden.

© BG ETEM 2024

Im Reiter „Neu hinzufügen“ wird folgender Dialog angezeigt:

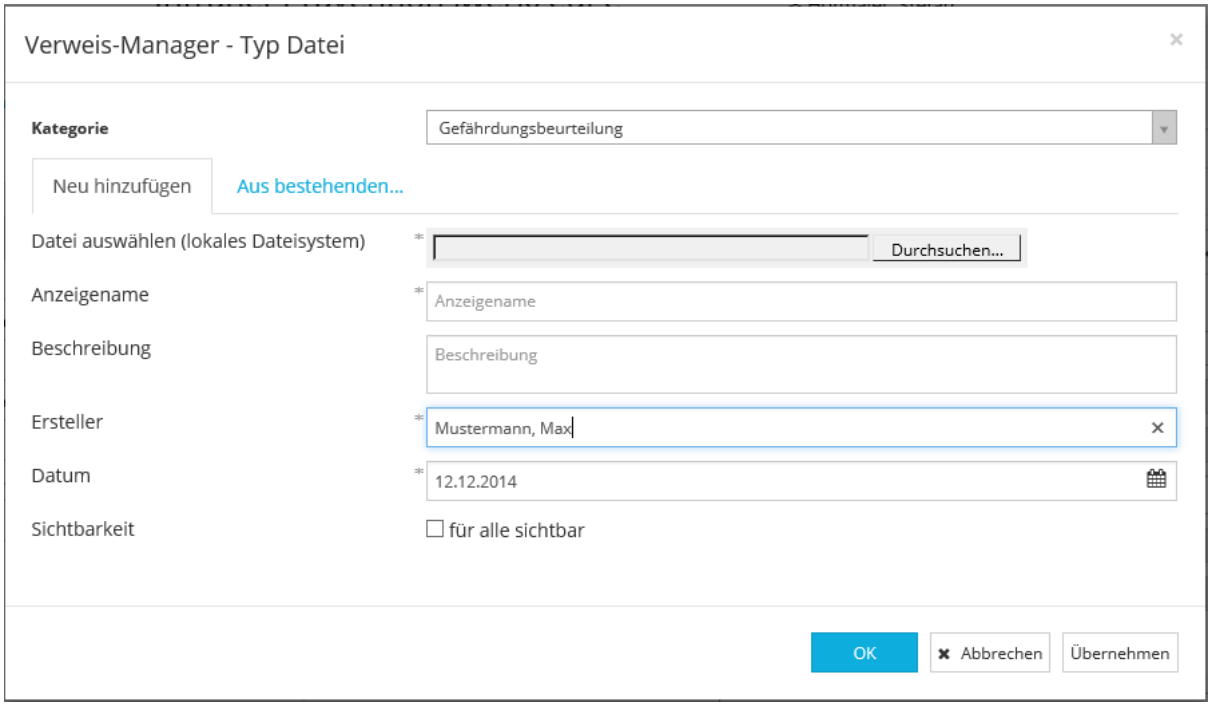


Abbildung 5: Verweis-Manager - Typ Datei

Im Feld „Kategorie“ kann die Kategorie der neu hinzuzufügenden Datei ausgewählt werden. Anschließend können für jede Kategorie beliebig viele Dokumente aus dem lokalen Dateisystem in das Medienverzeichnis übertragen werden. Für jedes Dokument müssen die sog. Metadaten befüllt werden. Durch Klicken auf die Schaltfläche „Übernehmen“ wird die aktuell ausgewählte Datei ins Medienverzeichnis kopiert. Anschließend kann das nächste Dokument ausgewählt und übertragen werden.

7.4 Migration strukturierter Daten aus anderen Quellsystemen

Analog zu der bereits verfügbaren Übernahme von Daten aus „Praxisgerechte Lösungen“ können im Rahmen eines Individualprojekts grundsätzlich auch Daten aus anderen Anwendungen und Datenquellen automatisiert nach „Intranet Präventionswerkzeuge“ übernommen werden.

Die in so einem Migrationsprojekt anzuwendende Vorgehensweise folgt einem standardisierten Verfahren, das in dieser Form auch für das oben beschriebene Migrationswerkzeug herangezogen wurde.

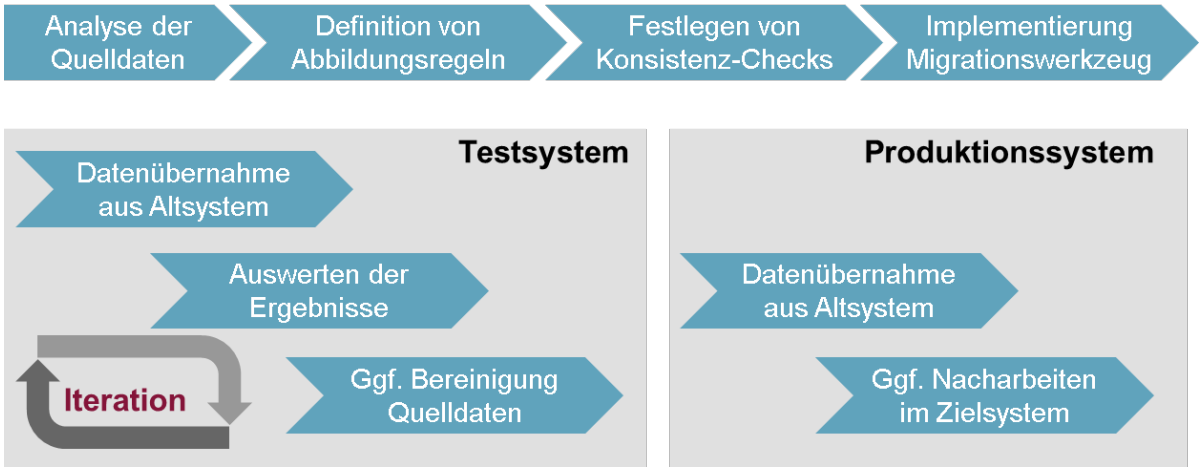


Abbildung 6: Standardisiertes Verfahren zur Migration von Daten aus anderen Anwendungen

Im ersten Schritt werden die zu migrierenden Quelldaten analysiert und festgelegt, welche dieser Daten nach „Intranet Präventionswerkzeuge“ übernommen werden können bzw. sollen.

Auf Basis dieser Ergebnisse sowie der detaillierten Kenntnis des Datenschemas und der Integritätsregeln von „Intranet Präventionswerkzeuge“ werden im nächsten Schritt Regeln für die Abbildung von Entitäten und Attributen des Quellsystems auf die Fachobjekte und Attribute von „Intranet Präventionswerkzeuge“ festgelegt. Zusätzlich muss über die Festlegung von Konsistenz-Checks und Akzeptanz-Kriterien sichergestellt werden, dass die Daten aus den Quellsystemen korrekt nach „Intranet Präventionswerkzeuge“ übernommen werden konnten.

Auf Basis dieser Festlegungen kann ein Migrationswerkzeug entwickelt werden, das die Daten aus dem Quellsystem analog zu dem Migrationswerkzeug für „Praxisgerechte Lösungen“ übernimmt.

Mit Verfügbarkeit des Migrationswerkzeugs wird in einem Testsystem die erste Datenübernahme aus dem Quellsystem nach „Intranet Präventionswerkzeuge durchgeführt. Die Auswertung der Ergebnisse erfordert ggf. eine Bereinigung von Daten im Quellsystem oder eine Anpassung / Verfeinerung im Migrationswerkzeug. Diese Schritte werden in mehreren Iterationen so lange ausgeführt, bis die vereinbarten Akzeptanzkriterien erfüllt sind.

Anschließend wird die produktive Migration der Daten durchgeführt. Zur weiteren Verbesserung der Datenqualität können bei Bedarf noch Nacharbeiten innerhalb von „Intranet Präventionswerkzeuge“ durchgeführt werden.

Die nachfolgende Abbildung skizziert den Ablauf einer Migration:

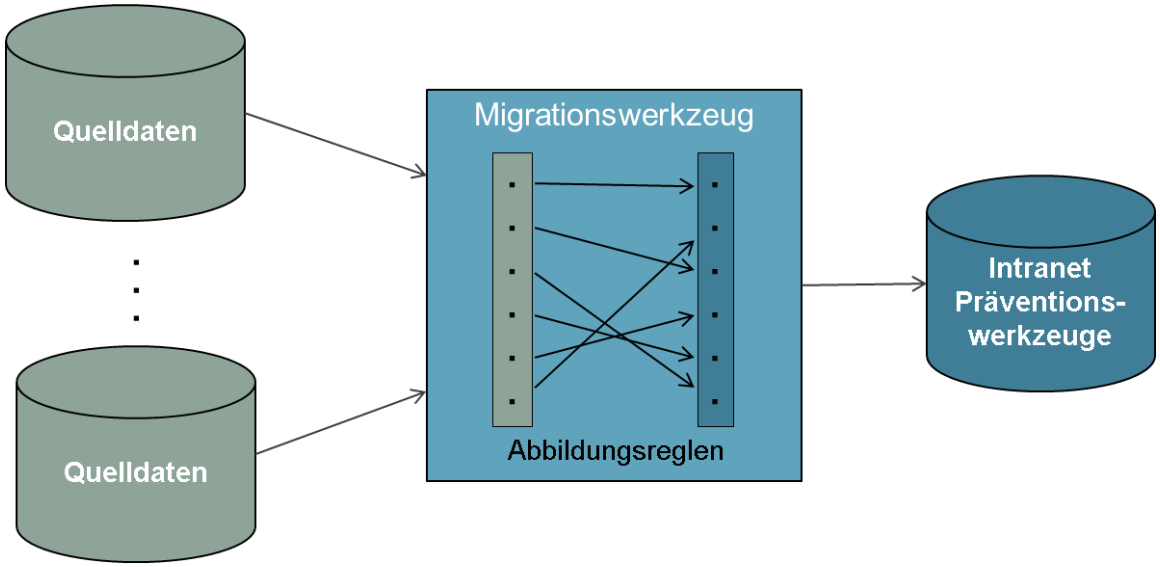


Abbildung 7: Ablauf einer Migration

8 Mögliche Fehlersituationen und deren Lösung

8.1 Fehlermeldungen in der Datei ipw.log

Grundsätzlich werden alle Fehler im Applikations-Log ipw.log gemeldet. Diese befindet sich standardmäßig im Verzeichnis:

```
ipw/gf.domains/ipw-domain/logs
```

Ein Fehler ist durch den Text "ERROR" nach dem Zeitstempel gekennzeichnet. Meist folgt danach ein relativ langer StackTrace der Anwendung, der anzeigt, bei welchem Aufruf bzw. Codestelle der Fehler in der Anwendung aufgetreten ist.

Beispiel eines Fehlereintrags (ohne StackTrace):

```
10-12-2014 14:12:27.178 ERROR [admin1] [GV] [MTQxODIxNzE0NjkwM2RlbGV0ZUdlZm-
FocnN0b2ZmMjM=] [com.msg.bgetem.ipw.rest.util.ErrorInterceptor] - EJBAccessExcep-
tion
```

Wesentliche Informationen sind der Zeitstempel des Eintrags und der Benutzer, dessen Aktion den Fehler ausgelöst hat. Auf Basis dieser beiden Informationen ist es möglich, die Fehlermeldung, die ein Benutzer angezeigt bekommt, und den Logeintrag einander zuzuordnen.

Nach dem angemeldeten Benutzer folgt das Modul, in dem der Fehler aufgetreten ist:

GV - Gefahrstoffverzeichnis

BA - Betriebsanweisung

VW - Basis

GB - Gefährdungsbeurteilung

RW - Regelwerk

MV - Medienverzeichnis

UM - Unfallmanagement

Ein Hinweis auf die auslösende Benutzeraktion ist im folgenden Schlüssel enthalten, im obigen Beispiel:

```
[MTQxODIxNzE0NjkwM2RlbGV0ZUdlZmFocnN0b2ZmMjM=]
```

Dekodiert man den Schlüssel nach dem BASE64-Verfahren (z. B. http://www.base64decode.org), erhält man:

```
1418217146903deleteGefahrstoff23
```

Der Fehler ist also beim Löschen eines Gefahrstoffes im Modul "Gefahrstoff" durch den Benutzer admin1 am 10.12.2014 um 14:12:27 aufgetreten.

8.2 Glossar aller Fehlermeldungen

8.2.1 Fehlermeldungen des Backends (Server-Anwendung)

Folgende Fehler sind vom Backend initiiert. Unter dem Backend ist in diesem Kontext die Java EE Anwendung gemeint, die im Payara Application Server abläuft.

Hinweis: Die aufgelisteten Fehlertexte enthalten Platzhalter in der Form %(<Variablenname>)s. Variablenname steht für den Platzhalter, der zur Laufzeit mit dem konkreten Wert für das Objekt, bei dem die Fehlersituation aufgetreten ist, gesetzt wird.

© BG ETEM 2024

Fehlercode	Fehlertext	Erläuterungen/Behebung
1000	Bei Ihrer letzten Aktion ist ein technischer Fehler aufgetreten. Bitte wenden Sie sich an Ihren Administrator.	Siehe Fehlerbeschreibung
2001	Löschen des Gefahrstoffs %(anzeigename)s nicht möglich, da mit dem Gefahrstoff verbundene Betriebsanweisungen existieren.	Falls der Gefahrstoff trotzdem gelöscht werden soll, betroffene Gefährdungsbeurteilungen und Betriebsanweisungen ermitteln und dort die Beziehung zu dem Gefahrstoff löschen.
2002	Löschen des Gefahrstoffs %(anzeigename)s nicht möglich, da mit dem Gefahrstoff verbundene Gemische/Gemenge existieren.	Der zu löschende Gefahrstoff muss aus allen Gemischen/Gemengen entfernt werden, damit dieser gelöscht werden kann.
2003	Löschen des Gefahrstoffs %(anzeigename)s nicht möglich, da mit dem Gefahrstoff verbundene Gefährdungsbeurteilung existieren.	Der zu löschende Gefahrstoff muss aus allen Gefährdungsbeurteilungen entfernt werden, damit dieser gelöscht werden kann.
3001	Das Löschen der Betriebsanweisung %(anzeigename)s ist nicht möglich, da mit der Betriebsanweisung verbundene Gefährdungsbeurteilungen existieren.	Falls die Betriebsanweisung trotzdem gelöscht werden soll, betroffene Gefährdungsbeurteilungen ermitteln und dort den Verweis auf die Betriebsanweisung löschen
3002	Generierte Betriebsanweisungen können nicht durch den Verweismanager überschrieben werden. Bitte nutzen Sie dafür das Modul Betriebsanweisungen.	Betriebsanweisungen können nur durch das Modul Betriebsanweisungen generiert, aber nicht über den Verweismanager manuell ins Medienarchiv hochgeladen werden. Verwenden Sie die Dokumentenkategorie Muster-Betriebsanweisung.
3003	Eine Betriebsanweisung mit dem Anzeigenamen %(anzeigename)s existiert bereits.	Der Anzeigename einer Betriebsanweisung muss eindeutig sein. Bitte wählen Sie einen anderen Anzeigenamen.
4000	Bei Ihrer letzten Aktion ist ein technischer Fehler aufgetreten. Bitte wenden Sie sich an Ihren Administrator.	Ein technischer Fehler ist auf dem Server aufgetreten (wie z. B. nicht genügend Speicherplatz, fehlende Berechtigung auf ein Verzeichnis o.ä.). Details sind in der Datei ipw.log zu finden.
4001	Das Objekt konnte nicht in der Datenbank gefunden werden.	Das angeforderte fachliche Objekt mit dem angegebenen Schlüssel konnte nicht gefunden werden. Es wurde zwischenzeitlich gelöscht oder es handelt sich um einen Programmierfehler.

© BG ETEM 2024

Fehlercode	Fehlertext	Erläuterungen/Behebung
4002	Bei Ihrer letzten Aktion ist ein technischer Fehler aufgetreten. Bitte wenden Sie sich an Ihren Administrator.	Die ID eines fachlichen Objektes differiert zwischen URL und Request Body. Es handelt sich um einen Programmierfehler.
4003	Die Datei kann nicht gespeichert werden.	Eine zum Server hochgeladene Datei konnte nicht gespeichert werden. Ursache können fehlende Berechtigungen des Payara-Prozesses, fehlender Speicherplatz oder Sonderzeichen im Dateinamen sein. Details sind in der Datei ipw.log zu finden.
4004	Der Benutzer %(benutzerkennung)s ist nicht in der Benutzerverwaltung des Unternehmens (Verzeichnisdienst LDAP) vorhanden. Das Neuanlegen des Benutzers ist deshalb nicht möglich.	Überprüfen des eingegebenen Benutzerkürzels. Ggf. muss der Benutzer im Verzeichnisdienst LDAP angelegt werden.
4005	Der Benutzer mit dem Benutzernamen %(benutzerkennung)s konnte nicht am Verzeichnisdienst Ihres Unternehmens angemeldet werden. Bitte überprüfen Sie Benutzername und Passwort und versuchen Sie es erneut. Falls Benutzername und Passwort korrekt sind, wenden Sie sich bitte an Ihren Systemadministrator.	Ein Benutzer mit dieser Benutzerkennung und dem eingegebenen Passwort ist der Anwendung nicht bekannt. Das Passwort muss geprüft werden. Ggf. muss der Benutzer zuerst im LDAP angelegt werden.
4006	Der Logout konnte nicht erfolgreich durchgeführt werden.	Der Logout des Anwenders ist fehlgeschlagen. Details sind in der Datei ipw.log zu finden.
4007	Die Datei $(datei) existiert nicht. Bitte wenden Sie sich an Ihren Administrator.	Der Download einer Datei ist fehlgeschlagen, da die Datei zwar in der Datenbank eingetragen ist, aber im Medienarchiv nicht mehr vorhanden ist. Die Konsistenz zwischen Datenbank und den Dateien des Medienverzeichnisses muss überprüft werden.
4008	Bei Ihrer letzten Aktion ist ein technischer Fehler aufgetreten. Bitte wenden Sie sich an Ihren Administrator.	Die Serverfunktion zur Anzeige der Startseitenelemente wurde ohne Angabe der Landessprache aufgerufen. Es handelt sich um einen Programmierfehler. Details sind in der Datei ipw.log zu finden.

Fehlercode	Fehlertext	Erläuterungen/Behebung
4009	Der Suchstring ist nicht valide.	Der Suchstring der für die Suche im Regelwerk verwendet wurde ist nicht valide. Bitte beachten Sie die Suchsyntax in der Online-Hilfe.
4010	Sie sind bereits in einer anderen Sitzung angemeldet. Bitte beenden Sie zuerst Ihre andere Sitzung und melden sich dann erneut an.	Ein Benutzer kann nur an einer Arbeitsstation gleichzeitig angemeldet sein. Die Sitzung an der anderen Arbeitsstation muss zuerst beendet werden.
5000	Bei Ihrer letzten Aktion ist beim Aufruf der Servermethode %(methode)s ein technischer Fehler aufgetreten. Der Parameter %(parameter)s wurde nicht übergeben. Bitte wenden Sie sich an Ihren Administrator.	Beim Aufruf der Serverfunktion hat ein Parameter gefehlt, dessen Angabe zwingend erforderlich ist. Es handelt sich um einen Programmierfehler. Details sind in der Datei ipw.log zu finden.
5001	Bei Ihrer letzten Aktion ist beim Aufruf der Servermethode %(methode)s ein technischer Fehler aufgetreten. Der Parameter %(parameter)s ist ungültig. Bitte wenden Sie sich an Ihren Administrator.	Beim Aufruf der Serverfunktion wurde ein ungültiger Parameter übergeben. Es handelt sich um einen Programmierfehler. Details sind in der Datei ipw.log zu finden.
5002	Sie haben im Feld %(feldname)s einen zu langen Wert eingegeben, die maximale Feldlänge beträgt %(maxlen)s Zeichen. Bitte korrigieren Sie Ihre Eingabe	Die maximale Länge eines Feldes wurde überschritten. Dieser Fehler sollte normalerweise vom Frontend abgeprüft werden. Der Feldinhalt muss vom Anwender gekürzt werden.
5003	Sie haben im Feld %(feldname)s ein ungültiges Eingabeformat verwendet. Das erforderliche Format ist %(format)s. Bitte korrigieren Sie Ihre Eingabe	Der eingegebene Wert entspricht nicht dem geforderten Eingabeformat. Der Feldinhalt muss vom Anwender korrigiert werden.
5004	Das Feld %(feldname)s ist ein Pflichtfeld. Bitte geben Sie einen Wert ein.	Der Wert für ein Pflichtfeld wurde leer gelassen. Der Anwender muss das Feld befüllen.
5005	Bei Ihrer letzten Aktion ist beim Aufruf der Servermethode %(methode)s ein technischer Fehler aufgetreten. Die Tabelle %(tabelle)s ist nicht vorhanden. Bitte wenden Sie sich an Ihren Administrator.	Eine Datenbanktabelle konnte wider Erwarten nicht gefunden werden. Es muss geprüft werden, ob die genannte Tabelle in der Datenbank vorhanden ist. Ggf. handelt es sich um einen Programmierfehler oder Installation der Anwendung wurde nicht korrekt durchgeführt.

Fehlercode	Fehlertext	Erläuterungen/Behebung
5006	Bei Ihrer letzten Aktion ist beim Aufruf der Servermethode %(methode)s ein technischer Fehler aufgetreten. Der Inhalt des Feldes %(feldname)s der Tabelle %(tabelle)s ist nicht eindeutig. Bitte korrigieren Sie Ihre Eingabe.	In der angegebenen Tabelle wurden zu einem als eindeutig festgelegten Attribut mehrere Objekte gefunden. Der Anwender muss den Inhalt des Feldes korrigieren. Falls sich dadurch der Fehler nicht beheben lässt, handelt es sich ggf. um einen Programmierfehler.
5007	Beim Speichern der Daten in der Tabelle %(tabelle)s ist ein Fehler aufgetreten. Bitte versuchen Sie es noch einmal. Falls der Fehler weiterhin auftritt, wenden Sie sich bitte an Ihren Administrator.	Ein Update auf die angegebene Tabelle führte zu einem techn. Fehler. Details sind in der Datei ipw.log zu finden.
5008	Im Medienverzeichnis ist für den Anzeigenamen %(anzeigename)s und die Dokumentenkategorie %(fachlicher_typ)s bereits ein Eintrag mit diesem Anzeigenamen vorhanden. Der Anzeigename muss innerhalb der Dokumentenkategorie eindeutig sein. Bitte wählen Sie einen anderen Anzeigenamen.	Der Anzeigename einer Datei muss pro Kategorie eindeutig sein. Bitte wählen Sie einen anderen Anzeigenamen.
5009	Die Pflichtfelder der Unfallmeldung sind nicht gefüllt. Bitte befüllen Sie alle Pflichtfelder.	Siehe Fehlertext.
5010	Die Pflichtfelder des Verbandbucheintrags sind nicht gefüllt. Bitte befüllen Sie alle Pflichtfelder.	Siehe Fehlertext.
5012	Einer freigegebenen Unfallmeldung muss mindestens eine Gefährdungsbeurteilung zugeordnet sein.	Siehe Fehlertext.
5014	Einer Unfallmeldung muss mindestens ein Strukturbaumknoten oder eine Gefährdungsbeurteilung zugeordnet sein.	Siehe Fehlertext.
5015	Bei Ihrer letzten Aktion ist ein technischer Fehler aufgetreten. Bitte wenden Sie sich an Ihren Administrator.	Siehe Fehlertext.
5016	Die erweiterte Suchabfrage '%(query)s' ist nicht valide. Konsultieren Sie die Hilfedokumente	Siehe Fehlertext.

Fehlercode	Fehlertext	Erläuterungen/Behebung
	für Informationen über das Format der erweiterten Suche.	
6000	Die von Ihnen bearbeiteten Daten der Tabelle %(tabelle)s wurden zwischenzeitlich durch einen anderen Benutzer überschrieben. Bitte starten Sie Ihre Bearbeitung neu.	Siehe Fehlertext.
6001	Der Datensatz mit dem Schlüssel %(id)s wurde in der Tabelle %(tabelle)s nicht gefunden. Bitte wenden Sie sich an Ihren Administrator.	Ein fachliches Objekt konnte wider Erwarten nicht gefunden werden. Entweder wurde es zwischenzeitlich gelöscht oder es handelt sich um einen Programmierfehler.
6002	Beim Zugriff auf die Datei %(datei)s ist ein Fehler aufgetreten. Bitte versuchen Sie es noch einmal. Falls der Fehler weiterhin auftritt, wenden Sie sich bitte an Ihren Administrator.	Eine Dateioperation (Lesen, Schreiben, Kopieren, Umbenennen) ist fehlgeschlagen. Details sind in der Datei ipw.log zu finden.
6003	Beim Lesen oder Speichern Ihrer Daten ist ein Fehler aufgetreten. Bitte versuchen Sie es noch einmal. Falls der Fehler weiterhin auftritt, wenden Sie sich bitte an Ihren Administrator.	Der Fehler basiert auf einer javax.persistence.PersistenceException oder java.sql.Exception und deutet auf einen Fehler im Zugriff von Java auf die Datenbank hin. Details sind in der Datei ipw.log zu finden.
6004	Das Löschen der Datei %(anzeigename)s ist nicht möglich, da die Datei in der Anwendung als Verweis referenziert wird.	Falls die Datei trotzdem gelöscht werden soll, müssen in der Anwendung alle Verweise auf die Datei gelöscht werden.
6005	Die von Ihnen geöffnete Aufgabe wurde zwischenzeitlich durch einen anderen Benutzer überschrieben. Bitte öffnen Sie die Gefährdungsbeurteilung neu, um einen Termin zu versenden.	Siehe Fehlertext.
7000	Die Konfigurationsdatei ipw-config.xml wurde nicht gefunden oder ist ungültig. Bitte wenden Sie sich an Ihren Administrator.	Der Pfad auf die Konfigurationsdatei wird durch die Variable IPW_PROPERTIES_PATH im Payara-Server gesetzt. Die Datei ist entweder im Dateisystem am angegebenen Ort nicht vorhanden oder die Variable IPW_PROPERTIES_PATH wurde nicht definiert.

© BG ETEM 2024

Fehlercode	Fehlertext	Erläuterungen/Behebung
7001	Der Pfad zur Konfigurationsdatei ipw-config.xml ist nicht korrekt gesetzt. Bitte wenden Sie sich an Ihren Administrator.	Der Pfad auf die Konfigurationsdatei wird durch die Variable IPW_PROPERTIES_PATH im Payara-Server gesetzt. Die Datei ist entweder im Dateisystem am angegebenen Ort nicht vorhanden oder die Variable IPW_PROPERTIES_PATH wurde nicht definiert.
7002	Die Sortierung der Gefährdungen ist nicht korrekt konfiguriert. Bitte wenden Sie sich an Ihren Systemadministrator.	In der ipw-config.xml wird die Sortierung der Gefährdungen unter dem Punkt Gefaehrdungsbeurteilung/SortGefaehrdungBy konfiguriert. Mögliche Werte sind erfassung, bezeichnung und faktor.
8000	Beim Zugriff auf den Verzeichnisdienst Ihres Unternehmens ist ein Fehler aufgetreten. Bitte versuchen Sie es noch einmal. Falls der Fehler weiterhin auftritt, wenden Sie sich bitte an Ihren Administrator.	Beim Zugriff auf den LDAP-Server gab es eine javax.naming.Exception. Details sind in der Datei ipw.log zu finden.
8001	Der Benutzer mit dem Kürzel %(benutzerkennung)s ist im Verzeichnisdienst Ihres Unternehmens nicht vorhanden. Bitte prüfen Sie Ihre Eingabe und versuchen Sie es noch einmal. Falls der Fehler weiterhin auftritt, wenden Sie sich bitte an Ihren Administrator.	Der angemeldete Benutzer konnte nicht mehr zum Abgleich der Benutzerdaten im LDAP gefunden werden. Vermutlich wurde der Benutzer gelöscht oder gesperrt.
8003	Der Benutzer %(benutzerkennung)s ist bereits in Intranet Präventionswerkzeuge vorhanden. Bitte überprüfen Sie Ihre Eingabe.	Betrifft die Neuanlage eines Benutzers. Siehe Fehlertext.
8004	Beim Versenden einer E-Mail an den Benutzer %(benutzerkennung)s ist ein Fehler aufgetreten. Bitte informieren Sie Ihren Systemadministrator.	Der E-Mail-Versand über SMTP hat einen Fehler gemeldet. Details sind in der Datei ipw.log zu finden.
8005	Beim Erstellen einer E-Mail an den Benutzer %(benutzerkennung)s ist ein Fehler aufgetreten. Bitte informieren Sie Ihren Systemadministrator.	Die Mail-Vorlage muss überprüft werden. Details sind in der Datei ipw.log zu finden.
8006	Beim Erstellen des Dokuments %(dokumentname)s ist ein Fehler aufgetreten. Bitte	Bei der Generierung eines PDF-Dokumentes hat das darunterliegende Framework JasperReports einen Fehler

Fehlercode	Fehlertext	Erläuterungen/Behebung
	versuchen Sie es noch einmal. Falls der Fehler weiterhin auftritt, wenden Sie sich bitte an Ihren Administrator.	gemeldet. Details sind in der Datei ipw.log zu finden.
8007	Beim Erstellen des Dokuments %(dokumentname)s ist ein Fehler aufgetreten. Die Dokumentenvorlage %(vorlage)s wurde nicht gefunden. Bitte wenden Sie sich an Ihren Administrator.	Bei der Generierung eines PDF-Dokumentes wurde die PDF-Vorlage nicht gefunden. Details sind in der Datei ipw.log zu finden. Ggf. muss die Vorlage aus der Sicherung wiederhergestellt werden.
8008	Die Suche im Regelwerk kann nicht ausgeführt werden, weil der Index der Suchmaschine defekt oder nicht verfügbar ist. Bitte wenden Sie sich an Ihren Administrator.	Vor der erstmaligen Verwendung des Regelwerks sollte der Index durch die GUI unter "Verwaltung ➔ Regelwerk indexieren" erzeugt werden. Wird dadurch das Problem nicht gelöst, so existieren Rechte- oder Platzprobleme auf dem Dateisystem.
8009	Es ist ein Fehler bei der Suche nach \"$(sqlquery)\" aufgetreten. Bitte passen Sie den Suchstring an.	Im Subsystem Apache Lucene ist bei der Ausfühung der Regelwerkssuche ein Fehler aufgetreten. Details sind in der Datei ipw.log zu finden.
8010	Der Benutzer mit dem Kürzel %(benutzerkennung)s wurde im Verzeichnisdienst Ihres Unternehmens gesperrt. Eine Anmeldung oder Bearbeitung ist deshalb nicht möglich.	Siehe Fehlertext.
8011	Der Benutzer mit dem Kürzel %(benutzerkennung)s ist im Verzeichnisdienst Ihres Unternehmens nicht mehr vorhanden und wurde deshalb in Intranet Präventionswerkzeuge gesperrt. Bitte löschen Sie den Benutzer aus Intranet Präventionswerkzeuge.	Siehe Fehlertext.
8012	Die Rolle %(rolle_name)s ist bereits in Intranet Präventionswerkzeuge vorhanden. Bitte wählen Sie einen anderen Namen.	Siehe Fehlertext.
8013	Das Löschen der Rolle %(name)s ist nicht möglich, da mit der Rolle verbundene Benutzer existieren. Die Liste der mit der Rolle verknüpften	Über die Benutzerverwaltung kann die Rollenzuordnung bei den entsprechenden Anwendern gelöscht werden.

© BG ETEM 2024

Fehlercode	Fehlertext	Erläuterungen/Behebung
	Benutzer wird nach Selektion einer Rolle angezeigt.	
8014	Das Löschen des Benutzers %(id)s ist nicht möglich, da Aufgaben für den Benutzer existieren oder der Benutzer als Verantwortlicher eines Gefahrstoffs im Gefahrstoffverzeichnis oder als Verantwortlicher einer Betriebsanweisung vermerkt ist.	Der Benutzer kann nicht gelöscht werden.
8015	Zur gewählten Sprache %(sprache)s wurden keine Dokumentvorlagen gefunden (Pfad: %(ordner)s). Bitte wählen Sie eine andere Sprache oder kontaktieren Sie Ihren Administrator.	Zur gewählten Sprache sind keine PDF-Vorlagen vorhanden, weshalb das Element nicht in dieser Sprache gedruckt werden kann.
9001	Bei Ihrer letzten Aktion ist ein Berechtigungsproblem aufgetreten.	Der Benutzer hat eine Serverfunktion aufgerufen, für die er keine Berechtigung besitzt. Es handelt sich vermutlich um einen Programmierfehler im Frontend.
9002	Beim Speichern der Daten für das Feld %(feldname)s ist eine Plausibilitätsverletzung aufgetreten. Bitte überprüfen Sie Ihre Eingabe.	Beim Löschen eines Benutzers oder Rolle ist ein Fehler aufgetreten, da Abhängigkeiten existieren (siehe auch Fehler 8013 und 8014).
9003	Die Gefährdungsbeurteilung %(gb_name)s kann nicht freigegeben werden, weil es zu dieser keine Arbeitsversion gibt..	Siehe Fehlertext.
9004	Die Gefährdungsbeurteilung kann nicht gelöscht werden, da mindestens ein anderes Dokument auf diese Gefährdungsbeurteilung verweist.	Soll die Gefährdungsbeurteilung trotzdem gelöscht werden, müssen die referenzierenden Gefährdungsbeurteilungen gesucht und der Verweis dort gelöscht werden.
9006	Die Gefährdungsbeurteilung %(gb_name)s kann im Status freigegeben nicht geändert werden, wenn es dazu eine Arbeitsversion gibt.	Siehe Fehlertext.
9007	Das System hat versucht, eine E-Mail an den Benutzer %(benutzerkennung)s zu senden. Das Senden der E-Mail	Die Aufgabe besitzt keinen gültigen Auftragnehmer (mehr). Der Benutzer muss

Fehlercode	Fehlertext	Erläuterungen/Behebung
	ist aber nicht möglich, weil der angegebene Benutzer nicht mehr in Intranet Präventionswerkzeuge registriert ist. Bitte lassen Sie den Benutzer in Intranet Präventionswerkzeuge anlegen und versuchen Sie es dann erneut.	erst in „Intranet Präventionswerkzeuge“ angelegt werden.
9008	Das System hat versucht, eine E-Mail an den Benutzer %(benutzerkennung)s zu senden. Das Senden der E-Mail ist aber nicht möglich, weil für den angegebenen Benutzer in Intranet Präventionswerkzeuge keine E-Mail Adresse hinterlegt ist. Bitte wenden Sie sich an Ihren Administrator.	Der Auftragnehmer der Aufgabe hat keine hinterlegte E-Mail-Adresse. Die E-Mail-Adresse muss im Verzeichnisdienst LDAP angelegt werden. Anschließend muss der Benutzer in „Intranet Präventionswerkzeuge“ bearbeitet und gespeichert werden.
9009	Bearbeitung einer Hauptversion mit Arbeitsversion nicht möglich.	Eine Hauptversion einer Gefährdungsbeurteilung kann nicht bearbeitet werden, solange eine Arbeitsversion existiert. Bearbeiten Sie stattdessen die Arbeitsversion.
9010	Gefährdungsbeurteilung befindet sich nicht im Status Freigegeben.	Arbeitsversionen können nur aus freigegebenen Version erstellt werden. Aus einer Arbeitsversion kann keine weitere Arbeitsversion erstellt werden.
9011	Der Eintrag kann nicht gelöscht werden, da er noch verwendet wird.	Der Auswahllisteneintrag kann nicht gelöscht werden, da er aktuell verwendet wird.
9012	Der Eintrag mit dem Schluessel %(schluessel) wird noch verwendet, da mindestens ein anderes Dokument dieses verwendet.	Der Auswahllisteneintrag kann nicht gelöscht werden, da er aktuell verwendet wird.
9013	Die erzwungene Freigabe ist aktiv und freigegebene Gefährdungsbeurteilungen können nicht bearbeitet werden. Bitte erstellen Sie eine Arbeitsversion und bearbeiten diese.	Die erzwungene Freigabe verhindert, dass eine freigegebene Gefährdungsbeurteilung bearbeitet werden kann. Dies Verhalten kann über die ipw-config.xml konfiguriert werden.
9014	Es kann keine Mail versendet werden, da für die gewünschte Massenbearbeitung der betroffenen Gefährdungsbeurteilung kein letzter Bearbeiter eingetragen ist.	Bei der Massenbearbeitung kann keine Mail versendet werden, da für die Gefährdungsbeurteilung des ausgewählten GB-Elements kein letzter Bearbeiter eingetragen ist und somit kein Empfänger für die Email vorliegt.
9999	Der Datensatz ist aktuell für die Bearbeitung durch einen anderen Nutzer gesperrt.	Der Datensatz ist als gesperrt markiert worden, weil ein anderer Benutzer diesen gerade bearbeitet. Hier gibt es mehrere Möglichkeiten: 1.) Den anderen Benutzer bitten, die

© BG ETEM 2024

Fehlercode	Fehlertext	Erläuterungen/Behebung
		Bearbeitung abzuschließen. Der Datensatz ist nun wieder verfügbar. 2.) Einen Benutzer mit dem Recht „Locks lösen“ bitten, den Datensatz zu entsperren.

8.2.2 Fehlermeldungen des Frontends (Client-Anwendung)

Folgende Fehlermeldungen werden vom Frontend initiiert. Mit Frontend ist in diesem Kontext der JavaScript-Code gemeint, der im Browser ausgeführt wird.

Fehlermeldung
Ein unbekannter Fehler ist aufgetreten.
Die Satz Stammdaten konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Die Symbol Stammdaten konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Die PSA Stammdaten konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Die Benutzer konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Die Rechte konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Die Rollen konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
BenutzerKnotenRollen-Objekte konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Der Strukturbaum konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Technische Probleme verhindern einen Login. Die Anwendung kann aktuell nicht genutzt werden. Bitte wenden Sie sich an den Systemadministrator.
Deine eigenen globalen Rechte konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Deine eigenen knotenbezogene Rechte konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.
Die Auswahllisten Stammdaten konnten nicht geladen werden. Die Anwendung wird nicht wunschgemäß funktionieren.

Allen Fehlern ist gemeinsam, dass die Verarbeitung sofort abgebrochen wird und die Anwendung nicht mehr wunschgemäß funktionieren kann.

Die wahrscheinlichste Fehlerursache für diese Meldungen ist, dass das Backend nicht erreichbar ist bzw. nicht ordnungsgemäß arbeitet. Folgende Punkte sollten geprüft werden:

© BG ETEM 2024

- **Ist der Payara-Server gestartet?**

  Unter Linux:

  Eingabe:

  ps -ef | grep payara

  Beispielhafte Antwort (es sollte ein Prozess gefunden werden):

  ipw-sw 2467 1 0 Dec08 ? 00:05:39 /v/ipw/sw/libexec/java-jdk17/bin/java -cp /……

  Unter Windows:

  Eingabe:

  asadmin list-domains

  Die Domaine ipw-domain sollte als running aufgeführt sein.

- **Ist die Datenbank gestartet?**

  Unter Linux:

  Eingabe:

  ps -ef | grep postgres

  Beispielhafte Antwort (es sollten mehrere Prozesse gefunden werden):

  ipw-sw-r 3977 1 0 Nov13 ? 00:00:07 /datafs/v/ipw/sw/bin/postgres -D /v/ipw/sw/var/postgresql/db -h 0.0.0.0 -p 5432 -k /v/ipw/sw/var/postgresql/run

  ipw-sw-r 4660 3977 0 Nov13 ? 00:00:02 postgres: checkpointer process

  ipw-sw-r 4661 3977 0 Nov13 ? 00:00:08 postgres: writer process

  ipw-sw-r 4662 3977 0 Nov13 ? 00:00:08 postgres: wal writer process

  ipw-sw-r 4663 3977 0 Nov13 ? 00:00:01 postgres: autovacuum launcher process

  ipw-sw-r 4664 3977 0 Nov13 ? 00:00:06 postgres: stats collector process

  ipw-sw-r 27916 3977 0 16:04 ? 00:00:00 postgres: bgetem_ipw_int bgetem_ipw_int 127.0.0.1(60436) idle

  Unter Windows:

  Prüfen, ob der Dienst postgresql unter den Diensten im Task-Manager im Status „Wird ausgeführt“ aufgelistet ist

- **Lässt sich die Testseite http://localhost:8080/ ipw-rest/v1/vw/hallo auf dem Server erfolgreich aufrufen?**

  Unter Linux:

  Eingabe:

  curl localhost:8080/ipw-rest/v1/vw/hallo

  Beispielhafte Antwort:

  {"anzahlDateien":21,"anzahlGefahrstoffe":55,"anzahlGefaehrdungsbeurteilungen":14193,"anzahlStrukturbaumKnoten":4609,"anzahlVerweise":2446,"anzahlMassnahme":75671,"anzahlGefaehrdungen":14567,"anzahlAufgaben":75637,"anzahlBetriebsanweisungen":34,"anzahlBenutzer":176}admin@msas6283i:~ [muellera@ps19]

  Unter Windows:

  Öffnen der Testseite mit Hilfe des Internet Explorers.

  Wurden alle Punkte erfolgreich überprüft, so sind die Logfiles server.log und ipw.log auf mögliche Fehler zu untersuchen.

8.3 Weitere bekannte Fehlersituationen und deren Behebung

Das folgende Kapitel gibt einen Überblick über mögliche weitere bekannte Fehlersituationen, die während des Betriebs der Anwendung auftreten können. Für Probleme bei der Installation der Anwendung beachten Sie bitte die Installationsanleitung.

Problem	Lösung
Bei der Suche nach Benutzern können keine Nutzer- Accounts gefunden werden.	Die LDAP-Verbindung, die für die Suche nach Nutzer- Accounts verwendet wird, wird in der ipw-config.xml konfiguriert. Bitte beachten Sie bei Problemen das server.log. In diesem findet sich ein LDAP-Error-Code. Die genaue Bedeutung des jeweiligen Codes lässt sich z. B. hier nachschlagen: http://wiki.servicenow.com/index.php?title=LDAP_Error_Codes Mögliche Fehlerquellen könnten z. B. sein: - Das Passwort in der Datei ipw-config.xml ist nicht BASE64 verschlüsselt - Das Passwort wurde mit einer Konsole verschlüsselt, weshalb ein führendes Leerzeichen mitverschlüsselt wurde. Verwenden Sie in diesem Fall https://www.base64encode.org/. - Der Benutzername entspricht nicht dem korrekten Format: username@realm also z. B. ipwadmin@test.com - Die Kommas innerhalb der BaseDN sind nicht durch einen Backslash maskiert - Der Benutzersuchfilter ist für Ihr Unternehmen nicht adäquat konfiguriert. Nach einer Änderung der ipw-config.xml muss der Server nicht neugestartet werden. Bitte beachten Sie ggf. auch die Groß- / Kleinschreibung der Nutzerdaten.
Der Login mit einem schon erfolgreich angelegten Nutzer- Account funktioniert nicht.	Die LDAP-Verbindung, die für den Login verwendet wird, wird in der domain.xml konfiguriert. Bitte beachten Sie bei Problemen das server.log. In diesem findet sich ein LDAP-Error-Code. Die genaue Bedeutung des jeweiligen Codes lässt sich z. B. hier nachschlagen: http://wiki.servicenow.com/index.php?title=LDAP_Error_Codes Mögliche Fehlerquellen könnten z. B. sein: - Das Passwort in der domain.xml ist BASE64 verschlüsselt - Der Benutzername entspricht nicht dem korrekten Format: username@realm, also z. B. ipwadmin@test.com - Die Kommata innerhalb der BaseDN sind durch einen Backslash maskiert - Der Benutzersuchfilter ist für Ihr Unternehmen nicht adäquat konfiguriert.

	Nach einer Änderung der domain.xml muss der Server neugestartet werden. Bitte beachten Sie ggf. auch die Groß- / Kleinschreibung der Nutzerdaten.

Die Migration bricht beim Migrieren der Strukturbaumknoten ab.	Bitte beachten Sie, dass für die Migration der „systemuser“ benötigt wird.
	Prüfen Sie innerhalb der Benutzerverwaltung der Anwendung, ob dieser vorhanden ist und über eine Rolle mit entsprechenden Bearbeitungsrechten verfügt („Rollen- und Knotenzuordnung von Benutzern bearbeiten“, „Strukturbaum verwalten“, „Benutzer verwalten“, „Gefährdungsbeurteilungen bearbeiten“).
	
	Sollte dieser nicht vorhanden sein, so lässt er sich nur über die Datenbank wiederherstellen. Dafür steht im „bin“ Ordner des PostgreSQL-Installation das Programm „psql“ zur Verfügung. Rufen Sie dies wie folgt auf:
	
	`psql –d ipw_database –U ipw_owner`
	
	Danach können Sie in der dann ausgeführten Datenbank-Konsole den “systemuser” erneut anlagen:
	
	`insert into vw_benutzer(version, benutzerkennung, intern) values (0, ‘systemuser’, false);`

Die Migration startet nicht.	Bitte prüfen Sie, ob der zu migrierende Katalog aus Praxisgerechte Lösungen Version 4 stammt. Sollte der Katalog aus einer älteren Version stammen, so müssen Sie zuerst die Anwendung „Praxisgerechte Lösungen“ aktualisieren um mit der dann aktualisierten „Praxisgerechte Lösungen“ den betrieblichen Katalog in den migrierbaren Versionsstand (≥4.0) zu konvertieren.
Auf einzelnen Rechnern werden keine Zeichen innerhalb der Funktionsschaltflächen im Internet Explorer dargestellt.	Nach unserer Recherche konnte hier der deaktivierte Schriftartendownload im Internet-Explorer verantwortlich gemacht werden. Mit hoher Wahrscheinlichkeit ist dieser für eine im Intranet betriebene Anwendung aktiviert. Sollte Ihr Internet Explorer jedoch keine Zeichen anzeigen, so stellen Sie bitte sicher, dass der Schriftartendownload für die Zone „Intranet“ aktiviert ist. Diese Option findet sich unter „Internetoptionen“ > „Sicherheit“ > „Stufe anpassen“.

Falls für die beschriebenen Fehlersituationen keine der vorgeschlagenen Lösungen zum Erfolg führt oder während des Betriebs der Anwendung ein anderes Fehlerbild auftritt, beachten Sie bitte Kapitel 9.

© BG ETEM 2024

9 Ansprechpartner bei nicht lösbaren Problemen

Im Fall eines Fehlers sollten, abhängig vom konkreten Fehlercode immer erst die relevanten Protokolldateien ausgewertet und die grundsätzliche Funktionsfähigkeit der Anwendung bzw. der einzelnen Systemsoftware-Komponenten (Webserver, Web Application Server, Datenbank) überprüft werden. Hierfür müssen auch die relevanten Konfigurationsdateien überprüft werden.

Für nicht lösbare technische oder fachliche Probleme stellt die BG ETEM den Mitgliedsunternehmen Unterstützung in Form einer Hotline zur Verfügung.

Die Hotline wird von der Firma msg systems betrieben und kann per E-Mail und per Telefon erreicht werden.

Mail-Adresse: **support-ipw@msg-systems.com**

Telefon: **089 / 96101-1102** (werktags von 9:00 – 17:00 Uhr)

Die Hotline ist für Administratoren und Multiplikatoren in den Mitgliedsunternehmen vorgesehen. Vor Kontaktaufnahme mit der Hotline sollten alle Informationen zu der Anfrage gesammelt und die bereits durchgeführten Analyseschritte dokumentiert werden. Die Fehlersituation sollte reproduzierbar sei. Bei Kontaktaufnahme per E-Mail ist es sinnvoll, Protokolldateien oder aussagekräftige Hardcopies von Bildschirminhalten gleich mit zu schicken.

© BG ETEM 2024